KWIC Index to GMIS POLICIES was compiled and edited by:

Ken Keen, GMIS 1st Vice President
IT Architect
Sedgwick County DIO/IT
538 N. Main
Wichita, KS 67203-3704
(316) 660-9858
kkeen@sedgwick.gov

This document prepared under the auspices of:

Bruce Miller, GMIS President
Salt Lake County
2001 South State Street, Suite S3200
Salt Lake City, Utah 84190-3300
(801) 468-3672
BWMiller@slco.org

and

Richard Vogt, CIO
Sedgwick County DIO/IT
538 N. Main
Wichita, KS 67203-3704
(316) 660-9851
rvogt@sedgwick.gov

This project was conceived because e-mail traffic on the GMIS listserv regularly asked questions similar to “Does anyone have a policy dealing with X?” (with X filled with the policy du jour). Usually there would be several replies with some of them being the “Me, too!” type. Others, with attachments, exhibited the spirit that drives the GMIS organization: cooperation among listserv members and a willingness to help one another. It occurred to me that compiling such submissions could make for a valuable document. Like anything needed though, such a compilation would be most useful if a needed policy could be quickly found. A couple of years ago, I wrote a small program (at home, on my own time Boss!) that takes text documents and creates a concordance of the text -- the word is shown in its context. Since not every word is worth putting out in this form, the program uses a small file to eliminate “junk” words (a, an, the, etc.). The key word is listed in a center column down the middle of the page with the context of the word on either side, I call the program KWIC – Key Word In Context.

As with most IT projects, this one deviated a little from what was envisioned. Instead of having the program search for EVERY instance of every key word, I selected only the first instance of the word within a policy. There is a consequence to this – if the word appears for the first time as a title heading, sometimes the context is not clear and it is even possible that just the word itself will appear without any context at all. The
excluded word list also doubled in size as I tried to cull out words upon which I believed no one would ever search. These changes mean the index is shorter (37 pages instead of well over 200) and hopefully more meaningful. I hope what we have is a good compromise of sacrificing excruciating detail for a more compact index.

I received the submissions in a variety of formats. To enable them to be used in the KWIC process, they have to be in .txt format. I have included the .txt version here, not the submitted format, so the original formatting, complete with logos, tabbing, numbering (in some cases), boxes, lines, headers/footers, and graphics has been lost.

No significant textual changes were made to the submissions. In a few cases, I have corrected errors in the original documents. Most of these were insignificant – spelling or a formatting issue. However, things like revisions and dates, related policies, signature lines for approval, page numbering, and names of approvers / signers / drafters have been omitted. Other than those, the submissions are intact.

I am grateful to those who made the effort to supply submissions to this project -- all 15 of you. I hope you benefit most! Their efforts truly manifest what GMIS is all about: sharing without an expected payback -- other than an answer to their possible call for help some time in the future. The project certainly could not have been as rich without you.

The results of the effort are here. I hope they will come in handy when needed.

Ken Keen
Editor
December 10, 2007

If you have a policy, and you don't enforce it, and you don't hold people accountable for violating it, then - do you have a policy?
# TABLE OF CONTENTS

 Preface ..................................................................................................................................................... 2
 GMIS SUBMISSION CONTRIBUTORS ......................................................................................................... 6
 HOW TO USE THE KWIC INDEX ............................................................................................................... 7
 CONTRIBUTED GMIS SUBMISSIONS ........................................................................................................... 8

 001 Portland Water District, ME – Acceptable Use Policy ............................................................................ 9
 002 Gaston County, NC – Acceptable Use Policy .......................................................................................... 11
 003 Charleston County, SC – Technology Usage Procedures ....................................................................... 29
 004 Martin County, FL – E-mail Acceptable Use Policy ............................................................................. 41
 005 Martin County, FL – Computing Resource Usage Policy ...................................................................... 44
 006 Martin County, FL – Desktop Computer Equipment Policy .................................................................. 49
 007 Martin County, FL – Computer Password Policy .................................................................................. 51
 008 Martin County, FL – Records Management Policy and Procedures ....................................................... 53
 009 Martin County, FL – Commodity Technology Purchasing Policy .......................................................... 72
 010 Martin County, FL – Global E-mail Distribution List Policy .................................................................. 73
 011 Martin County, FL – Cellular Telephones Policy .................................................................................. 74
 012 Village of Schaumburg, IL – After Hours Backup Policy ....................................................................... 76
 013 Village of Schaumburg, IL – After-Hours Computer Support Policy ..................................................... 77
 014 Village of Schaumburg, IL – Application Development Coverage Policy ........................................... 78
 015 Village of Schaumburg, IL – Customized Software Applications Policy .............................................. 80
 016 Village of Schaumburg, IL – E-mail Usage Policy .................................................................................. 82
 017 Village of Schaumburg, IL – Hardware Repair/Maintenance Policy ...................................................... 83
 018 Village of Schaumburg, IL – Hardware Standardization Policy ............................................................. 84
 019 Village of Schaumburg, IL – On-call Protocol ....................................................................................... 85
 020 Village of Schaumburg, IL – New Hire / Transfer / Move Requests Policy ........................................... 86
 021 Village of Schaumburg, IL – Problem Resolution Scenario ................................................................ 87
 022 Village of Schaumburg, IL – Organizational Strategy Policy ................................................................ 88
 023 Village of Schaumburg, IL – Equipment Replacement Policy .............................................................. 89
 024 Village of Schaumburg, IL – Requests for Equipment Policy ................................................................. 92
 025 Village of Schaumburg, IL – Office Equipment / Technology Replacement Policy ................................ 93
 026 Village of Schaumburg, IL – Security Systems Policy ............................................................................ 96
 027 Village of Schaumburg, IL – Software Licenses Policy ......................................................................... 97
 028 Village of Schaumburg, IL – Software Standardization Policy .............................................................. 98
 029 Village of Schaumburg, IL -- Telecommunications Policies and Procedures ......................................... 99
 030 Village of Schaumburg, IL -- Computer User Group Representatives Policy ..................................... 100
 031 Village of Schaumburg, IL – Web Site Link Guidelines and Procedures ................................................ 101
 032 Sedgwick County, KS – HIPAA Risk Analysis, Risk Management© .................................................... 102
 033 Sedgwick County, KS – HIPAA Information System Activity Review Policy© ...................................... 107
 034 Sedgwick County, KS – HIPAA Information Access Management & Workforce Security Policy© .... 108
 035 Sedgwick County, KS – HIPAA Security Awareness and Training Policy© ........................................ 110
 036 Sedgwick County, KS – HIPAA Security Incident Reporting and Response Policy© ........................... 112
 037 Sedgwick County, KS – HIPAA Security Contingency Plan Policy© ..................................................... 114
 038 Sedgwick County, KS – HIPAA Business Associates Policy© ............................................................. 116
 039 Sedgwick County, KS – HIPAA Facility Access Controls Policy© ....................................................... 117
 040 Sedgwick County, KS – HIPAA Workstation Use and Security Policy© .............................................. 119
 041 Sedgwick County, KS – HIPAA Device and Media Controls Policy© ................................................... 121
 042 Sedgwick County, KS – HIPAA Access Controls Policy© ................................................................. 122
 043 Sedgwick County, KS – HIPAA Audit Controls Policy© ............................................................... 124
 044 Sedgwick County, KS – HIPAA Security Policy© .................................................................................. 125
 045 Sedgwick County, KS – HIPAA Person or Entity Authentication Policy© ............................................ 126
 046 Sedgwick County, KS – HIPAA Transmission Security Controls Policy© ......................................... 127
 047 Sedgwick County, KS – HIPAA Security Officer Job Description ........................................................... 128
 048 Sedgwick County, KS – HIPAA Departmental Security Administrator Tasks .................................. 129
 049 Sedgwick County, KS – Data Center Security Policy .......................................................................... 130
 050 Sedgwick County, KS – Forensics Backup Procedure ......................................................................... 132
 051 Sedgwick County, KS – Information Technology Policy ..................................................................... 133
 052 Sedgwick County, KS – Acceptable Use Agreement ........................................................................... 137
 053 Sedgwick County, KS – Information Technology Usage Policy ............................................................ 138
 054 Sedgwick County, KS – Information Technology Usage Policy Procedures for Enforcement ............. 140
## GMIS SUBMISSION CONTRIBUTORS

<table>
<thead>
<tr>
<th>Policy</th>
<th>Contributor</th>
<th>Title</th>
<th>Jurisdiction</th>
<th>Phone</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Chad Davis</td>
<td>Network Administrator</td>
<td>Portland Water District, ME</td>
<td>(207) 523-5219</td>
<td><a href="mailto:cdavis@pwd.org">cdavis@pwd.org</a></td>
</tr>
<tr>
<td>2</td>
<td>Brandon Jackson</td>
<td>CIO</td>
<td>Gaston County, NC</td>
<td>(704) 866-3117</td>
<td><a href="mailto:brandon.jackson@co.gaston.nc.us">brandon.jackson@co.gaston.nc.us</a></td>
</tr>
<tr>
<td>3</td>
<td>Connie Berardinis</td>
<td>Director of Technology Services</td>
<td>Charleston County, SC</td>
<td>(843) 958-4025</td>
<td><a href="mailto:cberardinis@charlestoncounty.org">cberardinis@charlestoncounty.org</a></td>
</tr>
<tr>
<td>4-11</td>
<td>Kevin Kryzda</td>
<td>CIO</td>
<td>Martin County, FL</td>
<td>(772) 221-1310</td>
<td><a href="mailto:kevin@martin.fl.us">kevin@martin.fl.us</a></td>
</tr>
<tr>
<td>12-31</td>
<td>Sam Ferguson</td>
<td>Director of Information Technology</td>
<td>Village of Schaumburg, IL</td>
<td>(847) 923-380</td>
<td><a href="mailto:sferguson@ci.schaumburg.il.us">sferguson@ci.schaumburg.il.us</a></td>
</tr>
<tr>
<td>32-59</td>
<td>Ken Keen</td>
<td>IT Architect</td>
<td>Sedgwick County, KS</td>
<td>(316) 660-9858</td>
<td><a href="mailto:kkeen@sedgwick.gov">kkeen@sedgwick.gov</a></td>
</tr>
<tr>
<td>60</td>
<td>Sandy Rosenberg</td>
<td>Dir of Info Systems and Technology</td>
<td>Bloomfield, CT</td>
<td>(860) 769-3539</td>
<td><a href="mailto:sroenberg@bloomfieldct.org">sroenberg@bloomfieldct.org</a></td>
</tr>
<tr>
<td>61</td>
<td>George Curtis</td>
<td>Information Technologies Analyst</td>
<td>City of New Britain, CT</td>
<td>(860) 826-3445</td>
<td><a href="mailto:gcurtis@ch.ci.new-britain.ct.us">gcurtis@ch.ci.new-britain.ct.us</a></td>
</tr>
<tr>
<td>62-67</td>
<td>Craig Paull</td>
<td>Director, Information Technology</td>
<td>Kent County, MI</td>
<td>(616) 632-6501</td>
<td><a href="mailto:Craig.Paull@kentcountymi.gov">Craig.Paull@kentcountymi.gov</a></td>
</tr>
<tr>
<td>68-69</td>
<td>Wendy Rockwell</td>
<td>IT Director</td>
<td>Bradford County, PA</td>
<td>(570) 265-1720</td>
<td><a href="mailto:bcmis@mail.bradfordco.org">bcmis@mail.bradfordco.org</a></td>
</tr>
<tr>
<td>70-82</td>
<td>Dan Putnam</td>
<td>Information Systems Director</td>
<td>Livonia, MI</td>
<td>(734) 466-2150</td>
<td><a href="mailto:DPutman@ci.livonia.mi.us">DPutman@ci.livonia.mi.us</a></td>
</tr>
<tr>
<td>83</td>
<td>Bill Campbell</td>
<td>Network Manager</td>
<td>Salt Lake County, UT</td>
<td>(801) 468-3508</td>
<td><a href="mailto:bcampbell@slco.org">bcampbell@slco.org</a></td>
</tr>
<tr>
<td>84-89</td>
<td>Peter R. Hugret</td>
<td>Director Information Technology</td>
<td>Branford, CT</td>
<td>(203) 315-0617</td>
<td><a href="mailto:phugret@branford-ct.gov">phugret@branford-ct.gov</a></td>
</tr>
<tr>
<td>90</td>
<td>Bob Moyer</td>
<td>Director of Information Technology</td>
<td>Butler County, PA</td>
<td>(724) 284-1354</td>
<td><a href="mailto:BMoyer@co.butler.pa.us">BMoyer@co.butler.pa.us</a></td>
</tr>
<tr>
<td>91-98</td>
<td>Donald P. McCanless</td>
<td>Director of Information Technology</td>
<td>Montgomery, AL</td>
<td>(334) 241-2924</td>
<td><a href="mailto:dmccanless@montgomeryal.gov">dmccanless@montgomeryal.gov</a></td>
</tr>
<tr>
<td>99-106</td>
<td>Kevin Sweeney</td>
<td>Assistant Director of IT</td>
<td>St. Lucie County, FL</td>
<td>(772) 462-1759</td>
<td><a href="mailto:SweeneyK@stlucieco.gov">SweeneyK@stlucieco.gov</a></td>
</tr>
</tbody>
</table>
HOW TO USE THE KWIC INDEX

With the advent of computers with “find” options built into commonly available software (Word®, WordPerfect®, Excel®, Adobe Acrobat®) and remarkable “search engines” (Google®) that can find entries containing multiple words, it’s obvious that the KWIC Index is not as useful as it would have been before 1980. In some ways, what this document really offers is the collection of policies. It does provide the ability to see a volume of entries at a glance, or near-by entries that may trigger an idea.

USING THE INDEX

1. Search for a word of interest in the KWIC index at the back of this document.

2. If there are several entries for that word, use the context to the left and right of the word to make the best selection fitting the inquiry. Keep in mind that there may be multiple entries that actually fit what is wanted.

3. Make a note of the reference number at the right-hand end of the line.

4. The first number (to the left of the colon) is the number of the submission. Use either the Table of Contents or headings at the top of the pages to find the desired submission.

5. You may ignore the paragraph number to the right of the colon. You should read the entire document anyway. Remember, the KWIC Index was built selecting for the first instance of the key word, not each instance. But if you are into a larger document the paragraph number may give you a hint of where the word was found.

6. Regardless of the results of the work with the actual submission, remember that there were, probably, multiple entries for that word. Return to the index and try another entry and the submission to which it points.
CONTRIBUTED GMIS SUBMISSIONS
Purpose: The District’s objective is to ensure that proper use of the District’s computer and telecommunications resources and services by its employees, independent contractors, and other computer users. All computer users have the responsibility to use computer resources in an efficient, effective, ethical and lawful manner.

The following policy, rules and conditions apply to all users of computer and telecommunications resources and services, wherever the users are located. Adhering to the spirit of this policy should contribute to the safe and respectful environment necessary to carry out our mission. Violations of this policy may result in disciplinary action, including possible termination, and/or legal action.

Definitions: “Users” refers to all employees, independent contractors, and other persons or entities accessing or using The Portland Water District’s computer and telecommunications resources and services.

Scope: This policy applies to all District personnel.

Responsibility: The interpretation of this policy shall be the responsibility of the General Manager.

Policy:
The Portland Water District has the right, but not the duty, to monitor any and all aspects of the computer system, including employee e-mail, to ensure compliance with this policy. The computers and computer accounts given to employees are to assist them in the performance of their work. Employees should not have the expectation of privacy in anything they create, send or receive on the computer. The computer and telecommunication system belong to The Portland Water District and should be used for business related purposes.

Computer users are governed by the following provisions, which apply to all use of computer and telecommunications resources and services. Computer and telecommunications resources and services include, but are not limited to the following: host computers, file servers, workstations, stand-alone computers, laptops, software, and internal or external communications networks (Internet, commercial online services, bulletin board systems, and e-mail systems) that are accessed directly or indirectly from The Portland Water District’s computer facilities.

This policy may be amended or revised periodically as the need arises.

* * * Users must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property

* * * Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or other unlawful material may not be sent by e-mail or other form of electronic communication, or displayed on or stored in The Portland Water District’s computers. Users encountering or receiving such material should immediately report the incident to their supervisor.

* * * Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.

* * The user originating an e-mail will include the header “Confidential” or “Do Not Forward” when permission to forward has not been granted by the sender. User shall not forward e-mail to any other person or entity when the e-mail is marked as “Confidential” or “Do Not Forward” by the sender, unless such information is requested as part of an investigation.

* * E-mail from or to an attorney representing the company must include the following header on each page: “Attorney-Client privileged. Do not forward without permission.”

* * User are responsible for safeguarding their passwords for the system. Individual passwords should not be printed, stored on-line, or given to others. Users are responsible for all transactions made using their passwords.

* * The Portland Water District is not responsible for the actions of individual users.

A note about computer viruses:
A computer virus is a program designed to attach itself to another computer program. Some computer viruses damage the data on your disks by corrupting programs, deleting files, or even reformatting your entire hard disk. Most viruses stay active in memory until you turn off your computer. When you turn off the computer you remove the virus from memory, but not from the file, files, or disk it has infected. So, the next time you use your computer, the virus program is activated again and attaches itself to more
programs. As a precaution (and a matter of policy), you are advised to always scan disks for possible viruses before using them or when downloading files from bulletin boards. Users should not install software onto their individual computers or onto the network without first receiving express authorization to do so from a system administrator.

Development of computer skills:
The District encourages you to develop your computer use skills and to share your knowledge and abilities with others in order to enhance our overall ability to effectively meet customer needs. If you have an idea that will increase the effective use of computers, you are strongly encouraged to bring it to the attention of your supervisor or manager. We value your innovative ideas, and your personal development.

Complaint Procedure:
Any questions or concerns about this policy should follow the Union Grievance Procedure in the Union Contract or the Non-union compliant procedure in the Non-union employee handbook.
USE OF INFORMATION TECHNOLOGY RESOURCES

Introduction
1.1 Scope
All sections herein apply to employees, contractors, consultants, temporaries, and other workers at Gaston County including all personnel affiliated with third parties. These policies apply to all technology hardware and software that is owned, leased, or otherwise operated by Gaston County. The equipment includes but is not limited to: computer equipment, operating system software, application software, network accounts providing electronic mail, voice-mail, World Wide Web browsing, File Transfer Protocol, networking and intra-net hardware and software (collectively “System(s)”), that are owned by, leased, or licensed to Gaston County. The scope of this policy also includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Gaston County facility, has access to the Gaston County network, or stores any non-public Gaston County information.

1.2 Personal Use
Gaston County invests in and uses computer assets (computer hardware, software, supporting infrastructure, network-connections and telecommunications equipment) to support its business operations. Any personal use of these technologies should not create additional costs for Gaston County, interfere with work duties or violate any personnel policies, including policies related to defamatory, offensive or threatening messages, gambling, pornography, viruses, chain letters, personal shopping, executable 'ready to run files', "hacking", etc.

1.3 Intellectual Property Rights
All users should be aware that any information, software, or graphics on the Internet may be protected by federal copyright laws, regardless of whether a copyright notice appears on the work. Licensing agreements may control redistribution of information from Gaston County's Internet-related Systems or from the Internet. Duplication or transmission of such material or downloading shareware may not be undertaken without express authorization from IT.

1.4 Violation of Policy
Any violation or non-adherence to this Policy may lead to appropriate disciplinary action, as specified under previous policies of the Gaston County Personnel Policies and Procedures Manual, and/or suspension of Gaston County network resource access. In some cases such as theft of equipment or violation of copyright laws, violators may also be subject to civil and criminal process. To preserve the security and availability of Gaston County computing environments, system, network, and/or Internet access may be revoked.

2 Computer and Technology Use
2.1 Privacy
2.1.1 Purpose
Gaston County provides its employees the necessary computer and telecommunications equipment to assist them in the performance of their jobs. The following policy applies to all users of these Gaston County technology-related assets.

2.1.2 Ownership and Privacy Expectations
County employees are advised that there is no reasonable expectation of privacy when using County computer technology or communication systems. Because of the need to protect the County’s network, management cannot guarantee the confidentiality of information stored on any network, computer, or communications device belonging to Gaston County. Gaston County’s users should be aware that the data they create on County technology or communications systems remains the property of Gaston County and is not private (unless the data is personal health information covered by HIPAA or other personnel information protected by other privacy laws) and usually can be recovered even though deleted by the user. Furthermore, information that is stored on County technology or sent via e-mail may be subject to disclosure pursuant to the North Carolina Public Records Law. All technology resources and all information transmitted by, received from and stored on Gaston County systems are the property of Gaston County and as such, are subject to inspection and monitoring.
2.1.3 Monitoring
Gaston County has the right, but not the duty, to monitor any and all aspects of the County’s electronic technology resources. For security and network maintenance purposes, authorized individuals within Gaston County’s Information Technology Department may monitor equipment, systems and network traffic at any time. Upon authorization by the County Manager, the Director of Information Technology or designee has the authority to access without notice: data, pager memory banks, email and v-mail boxes, and other employer provided electronic storage systems. Gaston County reserves the right for business and security purposes to audit and monitor the information on all systems, electronic mail and information stored on computer systems or media, without advance notice. The County reserves the right to monitor all employee usage to ensure proper working order, appropriate use by employees, the security of Gaston County data, and to retrieve the contents of any employee communication in these systems. This might include investigation of theft, unauthorized disclosure of confidential business or proprietary information, personal abuse of the system or monitoring workflow and productivity. The County may access user files, including archived material of present and former employees without the user’s consent for any purpose related to maintaining the integrity of the network, or the rights of Gaston County or other users to ensure compliance with the County’s Information Technology Policies.

2.2 Computer Installation and Use

2.2.1 Purpose
In order to help users in the performance of their jobs, Gaston County has provided certain computer resources including hardware, software, printers, network access, etc. Gaston County promotes technology use to more efficiently achieve departmental missions, goals, and objectives. The following rules and guidelines apply to use of these Gaston County assets.

2.2.2 Ownership of Equipment
Information processing related systems, including but not limited to: computer equipment, operating system software, application software, network accounts (collectively “System(s)”), are owned by or licensed by Gaston County. It is forbidden to install non-County owned or leased equipment on Gaston County networks, with the exception of outside vendors for the purpose of providing services to the County, such that installation of equipment is required to perform services. Information Technology must provide approval of installation of non-County owned or leased equipment and/or software.

2.2.3 Installation of Equipment
Installation of all computer or computer-related hardware and software is to be performed exclusively by Information Technology (IT) department staff or their designated contractor(s). The procurement of these items is covered by the Technology Procurement section of this policy. The installation and use of software is covered by the Software Installation and Use section of this policy.

2.2.4 Security
Resource security must be maintained, and users should take all reasonable precautions, including but not limited to: safeguarding their passwords, maintaining reasonable physical security around Gaston County equipment, and logging off unattended workstations. Users should always log off workstations when leaving them unattended. (This does not mean you should necessarily power off the system itself.). A user who is logged on to a networked computer is responsible for any activity that occurs from within that account or on that computer during that sign-on.

2.2.5 Prohibited Uses
The following is a list of examples of prohibited uses. It is not intended to be a comprehensive and complete list. Other uses not listed here may be deemed as prohibited.

* Any use that violates federal, state, or local law, or regulation is expressly prohibited.
* Knowingly or recklessly interfering with the normal operation of computers, peripherals, or networks is prohibited.
* Connecting unauthorized equipment to the network for any purpose is prohibited.
* Running or installing games on Gaston County computers is prohibited. Running or installing unauthorized software on Gaston County computers is prohibited.
* Copying of any software from Gaston County computers, for other than archiving purposes, is prohibited.
* Using Gaston County network to gain unauthorized access to any computer system is prohibited.
* The use of Gaston County Systems to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist or other offensive material (including messages, images,
video, or sound) is prohibited. The use of Gaston County Systems in such a way as to create an intimidating or hostile work environment is prohibited.

* Gaston County Systems may not be used to solicit for personal gain or for the advancement of a political or religious belief.

2.3 Software Installation and Use

2.3.1 Purpose

This section defines Gaston County's rules for installation and use of software on Gaston County PCs, PDAs, smart phones, servers, and other hardware.

2.3.2 Background

Computer software (computer programs, databases and related documentation) whether purchased from a supplier or developed by Gaston County, is protected by copyright and may also be protected by patent. Employees are expected to strictly follow the terms and conditions of the license agreements, including provisions not to copy or distribute materials covered by these agreements. These protected materials may not be reproduced for personal use.

Only software that has been reviewed and/or tested by Gaston County IT is approved for installation on Gaston County computer hardware. Approval is based on various criteria such as, but not limited to: existing software standards, business needs, impact to network performance, overall cost of implementation versus business return, and compatibility with existing hardware. Usage of said software must pertain to county business purposes. No personal software is to be kept on Gaston County computers.

2.3.3 Installation

All software to be installed on Gaston County hardware is to be installed by IT staff or an agent authorized by the IT department. The software media and related media will be inventoried and stored by the IT department.

2.3.4 Auditing

Audits of computer software and hardware will be performed periodically by IT staff in order to ensure County compliance with software licensing and use agreements. Unlicensed and/or unauthorized software will be removed.

2.4 Email and Instant Messaging Use

2.4.1 Purpose

This section establishes standards that will protect the public image of Gaston County, and ensures that electronic communication is professional in content and purpose.

2.4.2 Scope

This section covers appropriate use of any email or instant messaging sent from a Gaston County email address, or with any content representing Gaston County.

2.4.3 Prohibited Use

The Gaston County email system should not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Gaston County employee should report the matter to their supervisor immediately and or send a copy of the email to the email spam account spam@co.gaston.nc.us. Employees should not respond directly to these emails or open any attachments with these emails.

Gaston County resources are not to be used to access personal email accounts such as but not limited to Hotmail, Yahoo, etc. Use of external, web-based email systems is permitted if for Gaston County business use.

Sending chain letters or joke emails from a Gaston County email account is prohibited. These restrictions also apply to the forwarding of such mail received by a Gaston County employee.

2.4.4 Broadcast emails

Gaston County employees may not send out broadcast emails to other Gaston County employees without County Management approval. County Management approval is obtained from the Gaston County Assistant Manager and/or the Public Information Officer. Once approval is given, then a copy of the email as it is to be sent out is sent to EmailAdmin@co.gaston.nc.us. No broadcast emails will be allowed that are not County business related, or a matter of community interest.
Gaston County employees may not utilize Gaston County email systems for high-volume broadcasting email messages across the Internet. Gaston County resources are not to be utilized to host email listservs without planning and approval by the IT department.

2.4.5 Personal Use
Gaston County email systems are not to be used for personal gain or solicitation of any form. Email usage is limited only to Gaston County accounts. Email is not to be used to distribute personal attachments (pictures, graphics, software, etc.).

2.4.6 Monitoring
Gaston County employees should have no expectation of privacy in anything they store, send or receive via the county’s email system. Gaston County may monitor messages without prior notice.

2.4.7 Email Attachments
Email attachments that end in: .exe, .com, .bas, .vbe, .pif, .url, .zip are all blocked by the email server and will not be allowed into the County’s email system. Attachment size is limited to 10 megabytes. Email is not an appropriate or efficient method of file transfer. If larger files need to be transferred via the Internet, arrangements are to be made with IT. Personal use attachments are not permitted.

2.4.8 Instant Messaging
Instant messaging has grown in popularity as a way for people to immediately communicate with each other via the computer rather than using voice systems. Instant messaging software has become available for free use through various sites such as MSN, AOL and YAHOO. With this growth has come increased activity on the part of hackers and vandals who exploit weaknesses in these systems. Attackers have been able to install and execute their programs on target desktop machines. They have also been successful in implanting destructive self-propagating worms that could exploit any number of weaknesses in your desktop computer. These worms may not be detectable by anti-virus software. As a result, the use of free instant messaging systems, such as but not limited to those provided by AOL, MSN, Yahoo, etc. are not permitted on Gaston County computers.

2.4.9 Retention
Gaston County email is to be centrally retained by Information Technology for seven years.

2.4.10 Definitions
Chain email or letter - Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck, money, etc. if the direction is followed.

2.5 Internet Use
2.5.1 Purpose
Gaston County has provided access to the Internet for all employees that need access for business related purposes. This policy will establish rules for the appropriate usage of the Internet for Gaston County employees.

2.5.2 Scope
This section covers all areas related to the approved usage of the Internet for Gaston County to prevent tying up the County’s network with browsing traffic that may slow down County business such as product research, obtaining quotes, access to GIS and Tax information.

2.5.3 Prohibited Use
The Internet for Gaston County employees should not be used for personal gain such as fund raising, partisan political activity or lobbying for non Gaston County business related purposes. Using the Internet to access sites which promote hate groups, pornographic material or discriminate against people because of their political beliefs, disabilities, age, sexual orientation or national origin is also prohibited.

2.5.4 Business and Personal Use
Browsing on the County’s network to the Internet is acceptable in small limited amounts as long as it doesn’t interfere with County related business or work productivity. Acceptable Internet use may include checking local news and weather, insurance information related to the County’s insurance plan, and possibly driving directions. Excessive non-work related browsing is not acceptable. Employees are not allowed to visit hate group sites, or sites that are pornographic in nature or discriminate against ethnic groups. Gaston County employees are not allowed to play streaming audio or video on the County’s Network, unless for Gaston County business purposes. This utilizes capacity necessary for Gaston County work. Any employee that is reported abusing the browsing privileges will be subject to further disciplinary action.

Proper business related uses of the Internet on the County’s computers include: acquiring information on County-related business and getting quotes for products, conducting research on new technologies,
accessing databases and files, delivering services to clients, and conducting County business with outside vendors. Examples of proper County-related business on the Internet include retrieving quotes for purchases, researching and accessing information on other counties’ websites for comparison purposes and training for County-related purposes.

2.5.5 Monitoring
Generally, the first level of monitoring is at the supervisory level. But, Gaston County can and does at times monitor network traffic such as Internet browsing to evaluate the load on the County’s Network. This is done through specialized software that provides information such as the desktop computer name, the sites visited and the amount of time spent on those sites. Abusive use of the County’s network traffic via Internet browsing will be reported to supervisory staff of that County employee for further disciplinary action. Abusive use includes visiting prohibited sites and non-work related browsing habits as previously discussed throughout this policy.

2.5.6 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action per the Gaston County Personnel Policy.

2.5.7 Definitions
Spyware - Software that embeds itself onto the desktop computer and communicates back to a host site on a user’s Internet browsing habits, or allows an unauthorized user to gain control of a user PC, etc. One sign of a computer infected with Spyware is usually a slowdown in the computer.

2.6 Phone and Voicemail Use
2.6.1 Telephone Usage
Gaston County provides its staff with telephones for conducting official county business. County phone use should be restricted to official county business purposes, except for emergency and important telephone communications, such as child care needs, medical appointments, and other critical communications. Reasonable, infrequent personal use of the County’s telephone systems by employees is permitted, but should not interfere or conflict with official County business use. Personal long distance telephone calls should not be made, except on an emergency basis. Charges for any personal long distance calls must be reimbursed to the County by staff.

Staff should not access communications intended solely for another employee unless requested to do so by intended recipient, or directed to do so by management. Classified, confidential, sensitive, proprietary or private information or data must not be disseminated to unauthorized persons or organizations.

2.6.2 Voice Mail Usage
Voice mail is a Gaston County asset and a critical component of communication systems. The voice mail system is provided by the county for employees to facilitate the performance of their work and its contents are the property of Gaston County. Although the county does not make a practice of monitoring these systems, management reserves the right to retrieve the contents for legitimate reasons, such as to find lost messages, to comply with investigations of wrongful acts or to recover from system failure. Examples of voice mail misuse include the following and are prohibited:

* Obscene, profane or offensive material being transmitted over any County communication system. This includes, for example, messages, jokes, erotic material or forms which violate our harassment policy or create an intimidating or hostile work environment.
* Use of company communications systems to set up personal businesses.
* Breaking into the system or unauthorized use of a password/mailbox is prohibited.
* Broadcasting unsolicited personal views on social, political, religious or other non-business related matters is prohibited.
* Broadcasting to solicit to buy or sell goods or services.
* Unauthorized access to an individual’s mailbox.
* Voice mails older than 60 days should be deleted from the system.

2.7 Cell Phone Use
2.7.1 Purpose
It is the policy of Gaston County to provide cellular telephones to employees for business use when use of such telephones will increase the level of service provided to the County’s customers, increase the level of safety for the applicable County employee, reduce cost of providing services, and/or satisfy legal requirements.

2.7.2 Business Use
A County cellular telephone should be used for appropriate business purposes. Such use is defined to be appropriate when an employee must make a call related to furthering County operations, does not have access to a regular County telephone and the call cannot or should not wait until returning to the office. The County also encourages employees to be good citizens and use cellular telephones to report emergency situations to the appropriate authorities, using free cellular calls whenever possible (e.g., 911 or *HP).

County employees with County cellular telephones will also use them in accordance with Gaston County Commission Resolution No. 2000-299, REGULATION OF MOBILE TELEPHONE USE WHILE OPERATING A COUNTY VEHICLE, approved September 28, 2000.

2.7.3 Personal Use
Certain personal calls are permitted, but are reimbursable to the County. Calls of this nature are typically for the well-being of the individual or his/her immediate family or for personal business that requires immediate attention and the employee cannot otherwise get to a regular telephone. Personal calls of this nature on County cellular phones that incur costs above the regular operating costs for the cellular phone service must be reimbursed to the County. This also includes personal calls that may have been made using allotted (i.e., free or no-cost) minutes and that caused official business calls to incur a cost because there were no allotted minutes remaining. Costs for these personal calls along with all applicable charges must be reimbursed by the applicable employee to the County by the end of the month in which the detailed telephone bill is received by the department. Reimbursement will be made by the employee to reduce the charges to the cellular telephone line item.

2.7.4 Incoming Calls
The County discourages the disclosure of cellular telephone numbers to members of the public as the telephones are the property of the County and not of the employee. All incoming calls are discouraged unless the calls are part of the business operations of the employee and their respective Department Director specifically directs the employee to encourage incoming calls for such purposes.

2.7.5 Telephone Misuse
Cellular telephone use and charges will be regularly monitored by each department's Director and periodically audited by the County Finance Department. Any intentional, deliberate misuse of a County cellular telephone may result in, but is not limited to, one or more of the following actions: progressive discipline of the employee misusing the cellular telephone, the requirement of a telephone log to be maintained detailing all calls, the blockage of all incoming calls, the loss of the cellular telephone service and employee reimbursement for the cost of the personal telephone calls and associated charges.

2.7.6 Responsibilities
It is the responsibility of each department’s Director to review the detailed cellular telephone bill for the department each month. The Director should note telephone usage patterns for both individuals and the department. The Director will investigate any unusual or questionable patterns and will take any appropriate action based on such investigation. It is also the Director's responsibility to ensure that copies of the telephone bill detail for each telephone is provided to the applicable employee and that any required reimbursement is made to the County on a timely basis in accordance with the requirements set forth herein.

It is the responsibility of the employee assigned a cellular telephone to use such telephone in accordance with this policy. Upon receipt of a copy of the telephone bill detail each month, the employee is to review such bill and note any calls which require reimbursement to the County. Reimbursement for such calls will be made according to departmental procedures and will be made by the end of the calendar month in which the bill copy is received.

2.8 Media Reuse and Disposal
2.8.1 Purpose
The purpose of this section is to ensure that all digital media is properly recycled or disposed of for reasons pertinent to data security, software license protection, and in compliance with environmental regulation.

2.8.2 Guidelines
If a hard disk, tape, CD, DVD, ZIP disk, diskette, or other storage device can be re-used, users should erase the existing data from the device and continue to use it, or make it available for someone else to use. If the digital media is unusable, or is no longer needed, it should be sent to IT Operations for destruction.
Unusable hard disks will be completely erased using a disk sanitizer utility. If that is not possible, the disk should be physically scratched and/or damaged to render it unreadable by any device.

3

Security

3.1 Network and System Access

3.1.1 Purpose

System access is an important aspect of computer security. The purpose of this section is to establish a standard for requesting access to the network and computer systems. Access to the county’s network and AS/400s is limited to Gaston County employees (including contractors and vendors with access to Gaston County systems). They are responsible for taking the appropriate steps, as outlined below to protect and secure their user passwords

3.1.2 Procedure to Request Access

Request for access to Gaston County's network or computer systems must be submitted through a service request via the ACTION System and approved by the requesting department's director or the department’s designated person. The service request should clearly state the following:

* Employee name, department, location, phone number
* Specifically what systems access is needed
* What software applications are needed to be accessed (inquire/update/etc.)
* Justification for each above item
* Internet, Intranet, email requirements
* Word processing, spreadsheet requirements

NOTE: Failure to be specific may delay implementation. Giving an example of an existing user’s access as a model will facilitate a quicker implementation.

While requests can be processed quickly by IT on an emergency basis, normal turn-around is two (2) business days.

3.2 Passwords

3.2.1 Purpose

The purpose of this section is to establish guidelines for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3.2.2 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Gaston County's entire network. As such, all Gaston County employees (including contractors and vendors with access to Gaston County systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.2.3 General Password Guidelines

Passwords are used for various purposes - user level accounts, web accounts, email accounts, screen saver protection, and voice mail password. Since few systems need passwords which are only used once, County staff are required to choose strong passwords and follow these guidelines when creating new passwords. Pass phrases (multiple words strung together) are recommended for passwords.

* All passwords must be changed at least every 120 days.
* User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
* Passwords must not be inserted into email messages or other forms of electronic communication.

Never create weak passwords that have the following characteristics:

* The password contains less than eight characters
* The password is a word found in a dictionary (English or foreign)
* The password is a common usage word such as:
  o Names of family, pets, friends, co-workers, fantasy characters, etc.
  o Computer terms and names, commands, sites, companies, hardware, software.
  o The words “Gaston County” or any derivation.
  o Birthdays and other personal information such as addresses and phone numbers.
  o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  o Any of the above spelled backwards.
  o Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Create strong passwords that have the following characteristics:
* Contain both upper and lower case characters (e.g., a-z, A-Z)
* Have digits as well as letters e.g., 0-9.
* Are at least eight alphanumeric characters long, the first being an alpha character and at least one being numeric.
* Are not a word in any language, slang, dialect, jargon, etc.
* Are not based on personal information, names of family, etc.
* Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R" or "Tmb1Wllr" or some other variation.

NOTE: Do not use either of these examples as passwords!

3.2.4 Password Protection Standards

Do not use the same password for Gaston County accounts as for other non-Gaston County access (e.g., personal ISP account, etc.). Where possible, don't use the same password for various Gaston County access needs. For example, select one password for ISeries sign-ons and a separate password for other IT systems. Also, select a separate password for a network account and an e-mail account.

Do not share Gaston County passwords with anyone, including directors, co-workers or IT staff. All passwords are to be treated as sensitive, confidential Gaston County information.

* Don't reveal a password over the phone to ANYONE
* Don't reveal a password in an email message
* Don't reveal a password to supervisor
* Don't talk about a password in front of others
* Don't hint at the format of a password (e.g., "my family name")
* Don't reveal a password on questionnaires or security forms
* Don't share a password with family members
* Don't reveal a password to co-workers while on vacation
* Don't use the "Remember Password" feature of applications (e.g., Outlook or any e-mail application, browsers).
* Don't write passwords down and store them anywhere in your office.
* Don't store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
* Don't reveal your password to IT staff (unless you intend to change it afterward)

If an account or password is suspected to have been compromised, report the incident to the Information Technology Department and change all passwords immediately. Password cracking or guessing may be performed on a periodic or random basis by the Information Technology Department. If a password is guessed or cracked during one of these scans, the user will be required to change it.

If someone demands a password, refer them to this document or have them call someone in the Information Technology security area.

3.2.5 Application Development Standards

Application developers must ensure their programs contain the following security precautions. All applications:
* Should support authentication of individual users.
* Should not store passwords in clear text or in any easily reversible form.

3.3 Data Storage and Backups

3.3.1 Purpose

The purpose of this section is to provide guidelines for data storage and backup to ensure that adequate data recoverability exists for mission critical information.

3.3.2 Background

Accidents, computer equipment malfunction or failure and human error are the most common causes of data loss. In most cases, damaged or lost data cannot be restored at any cost. In any case, don't rely solely on a single copy of data stored on your PC, a file server, or any other media, if losing that data would hamper your ability to perform County business.

3.3.3 Data Storage

All users are strongly urged to store user-created data on IT-administered file servers in order to ensure that the data is backed up. Regularly scheduled backups are performed on all County servers. Information Technology does not back up, and is not responsible for data residing on an individual user
PC. If an employee chooses to store pertinent information on their PC’s hard drive, they are responsible for the backup of that data. Users may choose to create additional backup copies of their own.

3.3.4 Backups
The regularly scheduled backups of file servers, performed by IT staff, are not intended for restoring individual users’ data files, but rather for recovering from file system damage caused by hardware/software failure, and minor disasters such as power outages. The procedures used by individuals for creating additional backup copies will differ based on the value of the data assigned by the user, how frequently the data is modified, and other factors. A number of alternatives for storing backup copies of user data are available. For individual, small sized files, regular 3 1/2 inch diskettes are reasonable. For moderate numbers or sized files, CD/DVD disks are quite adequate. For users with very large amounts of data, special arrangements must be made with IT for backups.

3.3.5 User Responsibility
Every computer user is responsible for determining and communicating backup requirements to IT for critical, irreplaceable data files. Storing valuable data in off-site locations is highly recommended. Data stored on typical media such as disks, diskettes, tape, CDROM, can be damaged by heat, magnetic fields, oxidation, etc., so copies cannot be relied upon indefinitely. For some users and their data, the IT server backup procedures are adequate insurance for data recoverability. In other instances, these procedures are not adequate. It is the user’s responsibility to determine what constitutes adequate backup coverage for his or her data.

3.4 Physical Security
3.4.1 Purpose
Gaston County must comply with HIPAA security guidelines and other regulations regarding the physical security of its computers and related networks. In addition to HIPAA guidelines, there are ancillary conditions and situations that require additional security. A physical security policy will ensure that Gaston County is in compliance with all regulations, as well as protect against data theft or vandalism from outside sources.

3.4.2 Guidelines
* Access to the server room, disaster recovery site, phone switches, and other key infrastructure will be limited by lock with access granted to authorized personnel only.
* Media, such as daily and monthly backups, will be stored in a secure area with limited access.
* Log-in access to all servers and personal computers should be limited to authorized personnel.
* The level of access to servers and personal computers will be administered by the Information Technology Department based upon the tasks required of the individual user.
* Employees should log off of all personal computers at the end of each business day to limit access to data accessible from their workstations.
* Employees should secure all personal computer or terminal screens with password protected screen savers when away from or not using said device.
* Employees should not maintain a physical copy of any system passwords in unsecured locations.
* All computer hardware must be protected from fire and other natural environmental hazards.
* Employees should exercise precautions to make sure that their computer hardware is not exposed to dangers related to their specific use, i.e. accidental beverage spills, improper ventilation of air intakes, etc.

3.5 Information Systems Activity Review (Monitoring)
3.5.1 Purpose
This section describes the user monitoring procedures adopted by the IT Department in the administration of Gaston County networks.

3.5.2 Scope
The entire Gaston County Network is monitored by IT Network staff to ensure proper and efficient functioning of the County’s services and network infrastructure. Abnormal network traffic may be traced to individual workstations and/or users. This process is monitored at the direction of the Network Services Manager and administered by the Network staff.

3.5.3 Monitoring Guidelines
The monitoring of County Network Systems adheres to the following guidelines.
* All information contained within email messages are the property of Gaston County and are subject to monitoring. Network Security staff will be responsible for best efforts toward ‘blocking’ of unwanted emails (“spam”) through email filtering.
* Network tools may be used to monitor the Internet usage by County users. Sites that consume County internet bandwidth such as listening to radio or TV broadcast are prohibited on the County network. The Network Security Administrator will take measures to block such sites.
* During the process of reviewing network email logs for the purpose of ensuring system performance and integrity, any discovery of abuse by network security staff will be reported to IT management. Information Technology management will report the information to the supervisors and Human Resources in accordance with County Personnel policy.
* Network Security staff will establish automated enforcement of proper usage of the network based on appropriate use policies.
* Network Security staff will run audit logs and monitoring tools at the request of departments. Requests must be made through the IT Department Director and or the Network Services Manager. These reports will then be given to the requesting supervisor at the end of the review.

3.6 Reporting Violations

3.6.1 Scope

Every department should have procedures in place to monitor compliance with the Information Technology Policies within this document, to report violations (both by "insiders" such as employees and contractors and "outsiders" such as unauthorized visitors, trespassers and hackers). It is the responsibility of each technology user to remain diligent in the identification and reporting of technology policy violations. Staff should be aware of their environment and report any suspicious, abnormal or unnatural behavior or events to the Director of Information Technology or his designee.

4 Technology Procurement

4.1 Hardware and Software Standards

4.1.1 Purpose

The purpose of this section is to ensure that technology hardware and software used within Gaston County Government will serve the needed functionality as requested by the department, while being mindful of the requirements of our platforms, network, interoperability and serviceability. Gaston County IT will have the responsibility of maintaining current technology hardware and software standards. The primary goal of this policy is to provide efficiency and economic return on Gaston County technology investments through centralized management.

4.1.2 Hardware Standards

Publishing guidelines recommending standard PC hardware configurations is a never-ending task. Such detailed configurations become rapidly out of date and require frequent policy changes to keep them current. Because of this, current standards for hardware will be maintained on an ongoing basis by Gaston County IT Department. Since all technology procurement must be approved by the IT Department, the IT Department will make sure purchase requisitions meet current standards.

4.1.3 Software and Network Connectivity Standards:

The recommended software and network connectivity standards for office automation and e-government applications are presented in the table below. This table is subject to periodic change, by the Information Technology Department. The latest standards should be viewed on the Gaston County Intranet site.

<table>
<thead>
<tr>
<th>Area</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems (PC and server)</td>
<td>Microsoft Windows platform (W2K or better)</td>
</tr>
<tr>
<td>Mainframe and Operating System</td>
<td>IBM iSeries with OS/400</td>
</tr>
<tr>
<td>System Management Software</td>
<td>Microsoft System Management Server</td>
</tr>
<tr>
<td>Messaging and Collaboration Server Software</td>
<td>Microsoft Exchange Server, IPSwitch iMail</td>
</tr>
<tr>
<td>Office Automation Suite</td>
<td>Office Automation Suite</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>Microsoft Office</td>
</tr>
<tr>
<td>Calendaring/e-mail</td>
<td>Calendaring/e-mail</td>
</tr>
<tr>
<td>MS Outlook</td>
<td>MS Outlook</td>
</tr>
<tr>
<td>Word Processor</td>
<td>Word Processor</td>
</tr>
<tr>
<td>MS Word</td>
<td>MS Word</td>
</tr>
</tbody>
</table>

4/7/2008
Spreadsheets
MS Excel
Presentation Graphics
MS PowerPoint
Document Imaging/Management Software
DocuWare
Database Server Software
Microsoft SQL Server
E-Government Application Development and Support Software
Microsoft Servers (W2K or better), Visual Studio .NET, FrontPage, Internet Explorer Browser products, Dreamweaver, Formium, Adobe Acrobat Professional, GeneXus .NET,
AntiVirus Suites
Computer Associates
Network Protocol
TCP/IP
Network Topology
Switched Ethernet
GIS
ESRI4.1.4 Non-Standard Items
For technology items not listed in the standards above, the Gaston County IT Department has final approval authority before purchase and use on the Gaston County network, and establishes the current standard.
Such items include but are not limited to the following:
* Digital Cameras
* Video projectors for computers
* Scanners
* Printers (including all-in-one and multi-function)
* FAX devices
* PDA
* Pocket Computers
* All memory devices and accessories for the above items
4.1.5 Co-Approval Items
Items requiring consultation and co-approval by the Gaston County IT Department would be (but not limited to):
* Security devices for facilities that require computer control and maintenance
* Video surveillance devices that are computer/network interfaced
* Any device or system that requires computer/network interfaces
4.2 Procurement of Technology
4.2.1 Purpose
The purpose of this section is to ensure that all technology procurements serve the needed functionality required by the requesting department, while being mindful of the requirements of our platforms, network, and service ability. The overall goal of this process is to provide efficiency and economic return on Gaston County technology investments through centralized management by the Information Technology Department.
4.2.2 Scope
This section pertains to the procurement of software, computer hardware, peripherals, network equipment, and any other Information Technology equipment. This policy does not apply to items that are generally considered to be consumables. Items considered to be consumables include, but are not limited to: computer paper, toner, ink cartridges, staples, media, and bulbs.
4.2.3 Procurement
Software, hardware, and other technology equipment requests are subject to the IT approval process. Once the new equipment has been approved, the order process will take place. All technology equipment must be received by the IT department. Once the item has been received and inventoried, the equipment will be installed at the requested location. The Gaston County IT department will house and catalog all of the installation media and warranty materials.
The IT department will deploy new hardware and software to the requesting department and reclaim the hardware that is being replaced. The reclaimed hardware will be brought to the IT department for evaluation. If the reclaimed hardware is determined to be past lifecycle, it will be tagged as surplus to be disposed of by facilities management or electronically auctioned by IT. If the reclaimed hardware is determined to be within lifecycle, it will be refurbished and redeployed at the discretion of IT department management. If a department is having existing computer hardware replaced and wishes to have the existing hardware redeployed within the same department, that department should submit a new work order requesting the redeployment. If the existing hardware is determined to be within lifecycle and the request is approved by IT management, the hardware will be redeployed. There is no expectation of departmental ownership of computers, software, or other technology equipment. All such items and equipment are considered to be owned by Gaston County. Exceptions are only those provided for in Federal or State law.

4.2.4 Procurement Process

1. A need or requirement is determined by a requesting department for technology purchase.
2. An IT service request should be generated requesting the technology item(s) via the online ACTION system. All specifications and details that are available are to be made known in the service request.
3. IT may contact the external department for clarifications that may be needed about items requested. IT will then obtain quotes and prepare a requisition.
4. The requesting department will receive a requisition from IT showing the selected vendor and price. The department must approve this requisition by having the department director, or approved proxy, sign the requisition on the “department approval” line. It should then be returned to IT for final IT director approval. No requisitions for purchase of technology items will be accepted by the Purchasing Department without the IT prepared requisition with all authorizing signatures including the IT Director or his designee.
5. The requesting department will receive the requisition back with the final approval. At this point the external department will enter the requisition into the county purchase order system and assign appropriate account/project numbers to be charged. Unless mutually agreed upon by the IT and requesting departments, the ship-to location should always be the IT department for receiving, warranty registrations, and inventory purposes. The instructions below are on the requisition prepared by IT and should be followed:
   * DO NOT change “Ship to Department” to anything other than 4210 when entering this requisition. IT must receive these items. When entering this requisition, please enter the following on the Comment line on the entry screen: “Do Not Mail – return this PO to IT for FAXing”
6. Once entered into the system, the requesting department must forward the original requisition with all approving signatures to the Purchasing Department as they will not release a Purchase Order (PO) without it.
7. The Purchasing Department will forward the PO to the IT Department for processing with the vendor.
8. The requesting department will receive the items shortly after IT has registered warranties and inventoried them.

4.2.5 Exceptions
IT has a responsibility to support systems that are approved and ordered through the procurement process as outlined above. Although rare, there are “technology” purchases that IT cannot order and support. An example would be a facilities management system for security purposes that is computer controlled. IT should be involved in the planning and procurement of all technology decisions to avoid financial and functional incompatibilities from a technology standpoint.

4.3 Technology Vendor Management

4.3.1 Purpose
The Vendor Management section formalizes standards for using and managing technology vendors within Gaston County. It is critical that the Information Technology staff manage the selection of technology vendors to ensure that the County is receiving the value for which the vendor was hired to provide. IT must be consulted for all engagements of technology vendors for Gaston County.

4.3.2 Controls
IT management must have a clear set of long-term goals and objectives for outsourcing efforts. Outsourcing should be used:
   * For operations difficult to manage and staff
   * To supply talent/resources unavailable in the organization
* To reduce internal operational costs
* To free resources for other efforts
* To bring improvements and benefits on board faster

When selecting a vendor, the following items should be considered:
* Gaston County business requirements met
* System operation documentation
* Security required
* Service volume
* Reliability level required
* Performance evaluation criteria
* Service volume expandability
* Hours and days of service
* Facilities required by vendor
* IT contact person
* Vendor contact person
* Clients of vendor’s service
* Contacts for confirming vendor’s credibility
* Length of time vendor has been performing this service
* Overall stability of vendor organization

Managing a long-term vendor relationship requires identifying contractual agreements and maintaining a close management relationship. Review the following items at least annually:
* Processing Timeframes
* Management Reporting
* Ongoing Costs
* Conversion Costs
* Insurance Coverage
* Training
* Access to Financial Data
* Privacy Policy
* Uptime Percentages
* Security Controls
* Internal Controls
* Disaster Recovery/Backup
* Non Performance & error Resolution
* Dispute Resolution
* Support/Maintenance response time
* Support/Maintenance quality

4.4 Redistribution of Used PCs
4.4.1 Purpose
The purpose of this section is to define the steps taken when a department has a request for a used PC from the IT Department.

4.4.2 Re-Assignment Criteria
Because IT maintains a limited number of used PCs in its parts depot, extreme consideration is exercised before a unit can be reassigned to another department. Justification for reassignment is based primarily on the criticality of the business function provided and whether the PC in question is already targeted for replacement in the next refresh cycle. The needs of the requesting department must be of an emergency or immediate nature.

4.4.3 Request Process
Departments should make their request via a Service Request using the ACTION system. The request should be as detailed and specific as possible. If a unit is being replaced with the requested used PC, it should be identified by the IT inventory label; all software being utilized on the unit should be listed as well as any new or planned software. If a used PC is being requested for a user who has no PC, the required software needs of that individual need to be specified on the request (ie. Specific software packages, Internet access, email, Intranet, Word, network server access, etc.).

4.4.4 Approval
The request for a used PC will be assigned and reviewed by the appropriate IT staff. Determining factors will include hardware availability and suitability for the requesting department's operational needs. Reassignment of used equipment is at the discretion of the IT Director and his designees in keeping with the needs of Gaston County and the departments supported by IT.

4.5 Accepting Donated Hardware or Software

4.5.1 Purpose:
Gaston County departments may accept and use donated computer equipment from the private sector on an individual basis. The purpose of this section is to ensure that acceptance of donated equipment does not interfere with current county equipment, standards or products. It is also imperative that the County have resources available to operate, maintain and support these donated items once accepted.

4.5.2 Request for Acceptance of Donated Equipment
Departments should make their request to accept donated equipment to IT via the ACTION system. The request for acceptance of a technology donation must include a clear statement identifying the benefit(s) to be gained by accepting the offer; where the equipment will be located; what applications are to run on the equipment, etc.

4.5.3 Approval
Donations are subject to review for such factors as age of equipment, compatibility, maintenance requirements, and compliance with current hardware standards in use by the IT Department at the time of donation.

A donation may not be accepted if it would in any way give the appearance of a loss of impartiality - that the donation would lead a reasonable person to question the integrity of County programs or services. Based on this criteria, departments may not accept donations from donors with an interest in matters pending before the County, donors involved in any public controversy, grantees or grant applicants, contractors or bidders for procurement, licensees or license applicants, or entities that are members of an entity governed by Gaston County. The acceptance and use of donated equipment is not to be construed in any manner as a County endorsement of the equipment, manufacturer or donor.

The Director of Information Technology is responsible for the overall implementation of the Acceptance and Use of Donated Equipment section. He or his designees will be the final authority to accept or reject any item offered for donation.

5 Technical Support

5.1 Obtaining Technical Support

5.1.1 Purpose
The purpose of the Gaston County Information Technology Department is to provide our user departments with the highest level of support possible for their technology needs.

The Information Technology Department is divided into 4 support areas:
* Applications Development (includes GIS),
* Networking and Communications,
* Desktop Support
* HelpDesk

5.1.2 Accessing Information Technology Support

5.1.3 Business Hours
Customers can contact the Information Technology Department Helpdesk for technical support by telephone between the hours of 7:00 am and 7:30 pm Monday through Friday, excluding holidays at 704-866-3068.

5.1.4 Off Hour Support
The department has on-call HelpDesk staff available 24 hours a day, 7 days a week and they can be reached via pager at 704-865-0099 extension 0214. They will return your call and notify the appropriate staff as needed.

5.2 Technical Support Process
The support process is classified into 2 categories:
* Trouble Ticket
* Call Escalation

5.2.1 Trouble Ticket
Upon receiving a request through the Helpdesk, the detailed Trouble Ticket is entered into the ACTION Support Application (ACTION) and is assigned to the appropriate staff member. An initial telephone
contact will be made, and in many cases the problem may be resolved. If this is not possible follow-up with the requestor will occur within 4 working hours. The staff member assigned will document all resolutions related to the trouble ticket, which can be viewed by the trouble ticket requestor via the ACTION system. When the request has been resolved, an email will be sent to the requestor to notify them of the completion of the trouble ticket. Feedback about the solution for the reported problem, the level of satisfaction with the solution, and the timeliness of the solution will also be solicited.

5.2.2 Escalation Process
When the assigned Information Technology staff member cannot complete the Trouble Ticket and/or needs additional assistance, the support call status is escalated to another staff member. Sometimes problems can be extremely difficult to replicate and resolve. When a problem remains unsolved for over 24 hours, an internal escalation process will be started. The problem is automatically flagged in the support database and is brought to the attention of the appropriate group manager who will establish the reason for the delay and take the necessary action to expedite. If after 72 hours the problem is still not resolved it will be brought to the attention of the Divisional Manager who will ensure the highest priority from all staff involved is given.

The Information Technology Department strives to provide excellent customer support. The above goals are minimums; in real terms IT will achieve far better than these stated goals with many problems being fixed on first contact.

5.3 Information Technology Business Hours
5.3.1 Purpose
The purpose of this section is to inform the IT customer base of the hours of operation for Gaston County’s Information Technology Department.

5.3.2 Business Hours
The Information Technology Department has staff available onsite during the following hours:
7:00 am – 7:30 pm    Monday – Friday

The Helpdesk can be reached at 704-866-3068.

5.3.3 Off Business Hours
The department has on-call HelpDesk staff available 24 hours a day, 7 days per week. During non-onsite hours they can be reached via pager at 704-865-0099, PIN# 0214.

5.3.4 System Availability
The Department’s 3 iSeries (AS/400’s) are scheduled for uptime:
* Monday – Sunday with the exception of a three-hour window each night for backups

The Production iSeries (SystemD) backup schedule is as follows:
* Daily backups are scheduled for Tuesday through Saturday from 2:00 am till 5:00 am.
* Weekly backups are scheduled for Sunday from 12:00 am till 3:00 am.

The Development/Disaster Recovery iSeries (SystemA) backup schedule is as follows:
* Daily backups are scheduled for Tuesday through Saturday from 3:00 am till 6:00 am.
* Weekly backups are scheduled for Sunday from 6:00 pm till 9:00 pm.

The Data Warehouse iSeries (SystemC) backup schedule is as follows:
* Daily backups are scheduled for Tuesday through Saturday from 6:30 pm till 9:30 pm.
* Weekly backups are scheduled for Sunday from 6:30 pm till 9:30 pm.

With the exception of the iSeries schedule, the County’s network (email, Internet, Intranet) is available 24 x 7 unless prior notification in accordance with our Change Management Policy is provided to our customer base for pending system maintenance.

6 Personnel Changes
6.1.1 Purpose
The purpose of this section is to ensure that Gaston County IT Department is promptly notified when an employee leaves Gaston County’s employment. It is imperative that user access to core IT resources be revoked in a timely manner when employees depart.

6.1.2 Person(s) with Primary Responsibilities
Primary responsibility belongs to the supervisor, administrator and/or director of the employee leaving Gaston County.

6.1.3 General Directions
The supervisor, administrator and/or director of a terminated employee must notify Gaston County IT Department of the separation on or before the employee’s termination date so that account access can be
revoked upon the employee’s departure. They must notify the IT Department by submitting a service request to IT Support Services using the online service request system (ACTION). The request should provide the employee’s user accounts and other identifying information (name, department, personal computer name/location, etc). If an existing employee will be temporarily assuming some of the departing employee’s duties, the service request should indicate what changes to system authorizations are needed to allow that employee to function. Under no circumstances, should one employee use another’s credentials to access systems.

6.1.4 Specific Actions
Upon receiving the service request notifying IT of a terminated employee, IT will disable the employee’s account(s) access. No account will be deleted until final termination notice has been received from the Human Resources Department. Accounts disabled will include the following: iSeries (AS/400), Network, eMail, DocuWare, and various application accounts depending on where the employee worked and their job function.

7
Network
7.1 Network TCP/IP Port Access
7.1.1 Purpose
This section describes the procedures required to request network port access to Gaston County networks.
7.1.2 Request Process
Requests for network port access must meet the following guidelines:
* Any request to open firewall ports must be initiated with a service request to the Information Technology Department via the ACTION system.
* The requesting party must justify opening of any outside ports and specify the length of time that these ports will be open and a date/time that they will be closed.
* All open port requests will be reviewed by the Network Services Group with a recommendation on approval/disapproval of port request. Their recommendation will then be reviewed and final approval will be made by the Network Services Manager and/or the IT Director. All open port requests must demonstrate a business benefit that outweighs the business risk.
* The network security administrator will perform test of opening ports and monitoring port activity before the implementation of opening the port. The Network Security Administrator will report the Network Services Manager on the benefits and possible problems with the requests and at that point the request could be denied.
* The Network Security Administrator will continue to monitor port activity. At the first instance of abuse of port activity the Network Security Administrator will report the abuse to the Network Services Manager and at that point the port may be closed.
7.2 Network Applications
7.2.1 Purpose
This section establishes the guidelines required to request installation of network applications. Any time a new application is introduced to a network, the addition can cause interruption of service to other applications.
7.2.2 Installation Criteria
The review, testing and approval of network applications are administered by Information Technology Network staff and must adhere to the following criteria:
* The service request for installation of network applications must be submitted to Gaston County Information Technology via the ACTION system.
* Network staff will review the application and determine the impact of installing the software on the network. The application must comply with Gaston County standards and run on the existing Gaston County network infrastructure. All software requests must be compatible and run on the established servers that are in production at the time of the request.
* Additional hardware required to run network software must be ordered, purchased and installed prior to loading the network software. It may be the requesting department’s responsibility to fund additional hardware or software requirements.
* Network staff will evaluate bandwidth requirements of the application. Installing the software in a test environment is preferred whenever possible.
* If a network IP Address is required, it must be assigned by the Network staff and will comply with the County’s IP addressing scheme.
* Remote access from software vendors will be under the control of the County’s Network staff. Access may be limited to certain times of the day and only for a certain amount of time.

8 Other Policies
8.1 Service Level Agreements

8.1.1 Purpose
A comprehensive service level agreement (SLA) is an essential requirement entered into between the Information Technology Department and customers for the provision or receipt of technology services. It defines the parameters for the delivery of that service, for the benefit of both parties. A well-defined SLA helps Information Technology promise what is possible to deliver and deliver what is promised. Performing as promised is important, but swift and well communicated resolution of issues is even more important.
The quality of the agreement is therefore a matter of substantial importance. It must be complete, comprehensive and accurate in its coverage. Importantly, both parties must understand the expectations, and their obligations.

8.1.2 Expectations
An SLA sets the expectations between Information Technology and the customer. It helps define the relationship between the two parties and is the cornerstone of how IT sets and maintains commitments to the customer.
A well-defined SLA addresses the following key aspects:
* What the provider is promising.
* How the provider will deliver on those promises.
* Who will measure delivery, and how.
* What happens if the provider fails to deliver as promised.
* How the SLA will change over time.
* Clearly defined customer commitments to assure that the internal processes follow the right direction.
* Performance indicators that can be integrated into a quality improvement process.
* Improving customer satisfaction remains a clear objective for IT staff.
* By tying the problem resolution process to an SLA, a service performance problem becomes an opportunity to structurally improve overall service quality and customer satisfaction, as opposed to just resolving the symptoms of the real issue.

8.1.3 Contents
Areas that must be defined in an SLA include:
* Description of the architecture and technologies that are used by the consumers of the service.
* Percentages of system uptime with details on how the measurements are done.
* Descriptions of specific services offered, hours of operation, system availability.
* What usage limitation the services have with regard to number of concurrent users as well as individual users.
* Details on how and who receives reports.
* Response times for inquiries – critical and non-critical (a non-critical inquiry is defined as a request for information that has no impact on the service quality if not answered or acted upon promptly).
* How conflicts are arbitrated.

8.1.4 Obligations
Obligations defined within the SLA must be realistic and measurable. An exponential relationship exists between the levels of availability and the related costs. Some customers require higher levels of availability with different associated costs; thus, the SLA must be defined within the confines of the technology infrastructure and budgetary constraints. As services and technologies change, the SLA may change to reflect the improvements and/or changes. All of the different internal groups within Information Technology (networking, operations, desktop support and applications) must commit to certain transaction response times to achieve the promised levels of service to the consumer.
Each SLA should be reviewed periodically and updated as necessary. Enhancements to the infrastructure, new users/customers, modifications to service measures, or changes to internal processes are examples of revisions that may be warranted in the SLA. When updates are deemed necessary, both parties will be asked to review and approve the changes.

8.2 Website Content Changes
8.2.1 Policy
Requests to update website content will be approved and implemented by Gaston County’s Public Information Office. This policy is limited to static content. Web-based applications fall under a separate policy.

8.2.2 Procedure
* Each department is solely responsible for the content of their respective website.
* All website content must comply with the Gaston County website standards (design, layout, etc.) as approved by the PIO.
* All information, if possible, must be submitted in digital format to webmaster@co.gaston.nc.us.
* The digital files should be in one of the following formats: Microsoft Office, Corel Suite, Adobe, rich text files, HTML, XML, ASP, ASPX, or JSP.
* Links to other websites are restricted to local, state, or federal government sites. Links to non-profit and personal websites are not allowed.
* Information on events will be limited to those directly sponsored by Gaston County.
* Each department will designate one person to act as the party responsible for sending the PIO website content updates. This person will be approved by the respective director of each department. Website content requests proposed by non-authorized personnel will not be considered.

8.3 Technology Policy Updates

8.3.1 Amendments
Gaston County may amend this Technology Policy from time to time as necessary. All users will receive prompt notice of any amendment.

8.4 Central Data Storage (insert after ‘Data Storage and Backups’)

8.4.1 Purpose
The purpose of this section is to provide guidelines for centralized data storage on Gaston County servers (AS400, Windows, Storage Area Network, Networked Attached Storage, etc.).

8.4.2 Background
While disk space continuously drops in cost, it is not free, and requires planning to procure, install, and maintain. It is not unusual for an organization to experience 50 to 100% annual data growth rates. As of January, 2006, Gaston County Information Technology was responsible for over 6 terabytes (TB) of central data. According to the growth rates described above, in 2011, Gaston County IT would manage between 45 and 192 TB of data.

8.4.3 User Responsibility
All new central data storage requirements (data destined for any central server, SAN or NAS) MUST be approved by IT. The purpose of approval is allow IT to verify that current and future capacity requirements are met, and determine the most effective, and cost-efficient means for storage. Requests for new data storage requirements should be submitted to IT via Service Request. For new data-related projects, Information Technology should be brought in as early in the process as possible (during the conceptual stage). Introduction of IT later in the process may cause preventable delays.

8.4.4 Storage Area Network (SAN)
While SAN solutions are efficient, and cost-effective in many circumstances, they are not in all circumstances. Gaston County IT has established the following criteria to prioritize use of SAN storage:

HIGH
- CRITICAL data (business will NOT operate without it)
- county-wide/multi-departmental data (e.g. SQL databases, email, enterprise app data)
- Data for DIRECT public service (GIS, Tax data directly visible to public via web)

LOW
- Single department data
- convenience archive data

SAN expansion requires an extra level of planning beyond the simple addition of hard drives. For this reason it is necessary for departments to evaluate their central data storage requirement needs on an annual basis, and present them to Information Technology before budget planning for the following year.
3 Introduction
In order to maximize the benefits of the technology investments across the Charleston County, the Technology Services group has created this document, “Technology Usage Procedures,” to address and communicate existing and new procedures. Goals of these procedures are:
2. Protect confidential, proprietary information of the county from theft or unauthorized disclosure to third parties;
3. Be cost-effective and prevent waste of technology resources;
4. Reduce, and if possible, eliminate, potential legal liability to employees and third parties.
The County requires that all new and existing employees sign a written statement that they have read these procedures and understand these guidelines.

3.1 Technology Services Vision Statement
Provide value-added technical services and solutions to Charleston County that enhance or enable better service to our citizens.

3.2 Mission
The County makes strategic use of information technology, to provide the most value to:
* Enable the employees to best serve their customers
* Deliver information and services to citizens at work, at home and in the community
* Increase the productivity of our services
* Increase citizen access to information

3.3 Goals
* Ensure the availability and security of our network
* Enable ease of obtaining and sharing of data.
* Lower costs - Achieve technology standardization where feasible
* Better enable disaster recovery of critical systems.
* Offer flexibility in the workplace

3.4 Guiding Principles:
* Technology Services will provide quality customer service and solutions.
* Technology Services will support employee well-being.
* Technology Services will demonstrate professionalism and be customer focused – to our citizens, County teammates, and business partners.
* Technology Services will maximize our information technology investment by leveraging our solutions and services to the fullest extent possible across the County.
* Technology Services will promote and implement standard technology and solutions, where feasible, throughout all County offices to support common business processes.
* Technology Services will use commercially available software packages wherever possible.
* Technology Services will work efficiently using best practices.

4 Communication
Technology Services will update these procedures, as needed, and once approved, will communicate the updates to all Department Heads and technology Contacts, as appropriate. Technology Services will also provide access to these procedures on the County Intranet site.
The County will use reasonable efforts to notify Users when software patches or other software is deployed to User PCs and where there may be a disruption to the User. There will be times where software will need to be deployed where prior notice may not be feasible, as in the case where there is a security risk or legal/statutory compliance requirement or where such deployment is transparent to the user, as in the case of operating system or application upgrades; asset inventory data collection, data collection for license management and compliance, or for new software that the county deploys and which can occur in the background without disruption to the User.

5 Standards
Technology Services has the responsibility for support and problem resolution for the County’s PCs. To effectively and efficiently carry out that role, Technology Services must be able to rely on standard
hardware and software configurations on the desktop. Users must request hardware and software through Technology Services.

5.1 Hardware Standards
The current standard hardware for use at the County is listed in the IFAS catalog and also provided on the County Intranet site. Department Heads who have a need to deviate from the standards must request an exception. The Director of Technology Services will review the request and either approve request as is, or suggest alternate solution to ensure support can be provided. If a satisfactory solution cannot be agreed upon, the issue will be raised to the appropriate member of the Management Team.

5.2 Software Standards
Technology Services must first acquire and test programs and executables before employees save them to their desktop computer. Software may only be used in compliance with the terms of the applicable license agreements.

The Software Standards specify the technologies supported by the organization and serves as a guideline for all technology purchasing and use decisions, including hardware, software, peripherals, and network components. Current software standards are listed on the County’s intranet site.

5.3 Unauthorized Software
Use of unauthorized software can degrade the county’s network and Internet service, create security risks and personal computer problems, divert focus from county-related issues, reduce employee productivity and increase costs. It is the responsibility of all Users in all departments to comply with maintaining the County standard by not downloading or installing unauthorized software onto any County owned PC or laptop. Any software which needs to be downloaded and installed is to be done by Technology Services. Unauthorized software is any software that is not approved for use by Technology Services to conduct the business of Charleston County.

Technology Services will 1) immediately remove the unauthorized software in use when encountered and 2) on a routine basis, check and remove unauthorized software, unless the software has a legitimate business purpose for the User. Technology Services will work with User departments to ensure any questionable software usage is addressed before removal.

6 Network Resource Usage – Internet, Email & Data
Access to and use of the network, Internet and/or e-mail systems is provided to employees of Charleston County for the purpose of advancing the goals of the County. This access imposes certain responsibilities and obligations on County employees, (full-time, part-time and temporary employees), officials, and as well as any companies or individuals (third parties) contracted to do work for the County, or use County technology resources, (hereinafter termed “Users”) and is subject to County government policies and local, state and federal laws. All data, e-mails, e-mail attachments, documents and other electronic information within the network/e-mail system are the property of Charleston County. THERE SHOULD BE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY IN NETWORK USE, INTERNET ACCESS AND E-MAIL USE ON THE COUNTY’S SYSTEMS. The County, acting through its managers and supervisors, has the capability and the right to view data and e-mail at any time when deemed necessary for County business purposes. These procedures do not supersede any state or federal laws regarding confidentiality and appropriate use.

The primary purpose for using the County’s network, Internet and e-mail connection is in advancing the business of the County. This includes, but is not limited to:
* Communication with, and providing service to, clients and citizens of Charleston County.
* Conducting the business of your department or unit
* Communicating with other employees for work-related purposes.
* Gathering information relevant to your duties or to expand your expertise.

Acceptable use always is lawful, ethical, reflects honesty, and shows restraint in the consumption of shared resources. Users shall refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer paper, manuals or other resources. Users may be subject to limitations on their use of the networks, or other action, as determined by the appropriate supervising authority. Users are also expected to cooperate with any investigation regarding the use of your computer or your activities associated with technology resources.

Content of all communications should be accurate. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.
As with internal e-mail messages, Internet e-mail can be changed by outside parties and forwarded to others without the employee’s knowledge or permission. Users must use caution in using Internet e-mail and must comply with all state and federal laws. Users should abstain from using County e-mail IDs in public forums / chat rooms, etc., as it can result in the increase of spam.

User data and documents are a County asset and should be treated as such. For this reason, Users who have access to a shared network drive should store all data files on the shared drive as these files are backed up daily. Recovery of data stored on desktops is the User’s responsibility. Storage only on a PC hard drive is a risk in that if the hard drive fails, the data may not be recovered.

6.1 Limited Personal Use

Authorized Users of the County may also use the Internet and e-mail for limited personal use. This is defined as any personally initiated online activity (including e-mail and Internet usage) that is conducted for purposes other than those listed above. This is a privilege, not a right, and may be limited or removed at any time by management. Charleston County does not accept liability for any loss or damage suffered by an employee as a result of that employee using the County Internet connection for personal use. Occasional, limited, appropriate personal use of the computer system is permitted when the use does not:
1. interfere with the User’s work performance (It shall be infrequent and brief.);
2. interfere with the normal operation of your department or work unit;
3. interfere with any other User’s work performance or have a negative impact on overall employee productivity;
4. have undue impact on the operation of the computer system;
5. cause any additional expense or load to the County or department;
6. compromise your department or the County in any way;
7. violate any other provision of these procedures, any other policy guideline, any law/regulation, i.e., HIPAA, or standard of Charleston County.

In limiting personal use, the County expects employees to exercise the same good judgment that they would use in all work situations. For example, you are expected to know that taking five minutes to call your spouse during a coffee break is acceptable, while taking three hours to go shopping at the mall during the workday is not. Making decisions about your use of Internet resources is no different. The examples below illustrate the kinds of situations where it is hoped employees would exercise good judgment. Examples provided below are not meant to be exclusive and are for illustration only:

Limited Personal Use Access Abuse
Alice keeps in touch with a circle of friends from high school via e-mail. Occasionally she will take a few minutes to read and respond to an e-mail from one of those friends.
Rob is the convener of a local amateur sports association. He has given his work e-mail out as his main contact. During the sports season, he spends up to 90 minutes each morning responding to queries and complaints, and otherwise conducting league business.
Nauman is a big fan of international cricket. During the world championships, he takes a few minutes every morning to check a Web site that carries the overnight scores from Asia.
Mike frequents Web sites that are clearly prohibited by the County’s acceptable use procedure. Coworkers have been offended by some of the images clearly displayed on Mike’s computer.
Mary reads a review in a magazine of a new novel by Stephen King. While at work the next day, she logs onto Amazon.com and purchases the book for delivery to her home address.
Todd needs a new fishing rod and spends over an hour browsing different models at a sporting goods Web site.

6.2 Inappropriate Use

The use of public resources for personal gain and/or excessive private use, such as but not limited to the items listed below, by any User is absolutely prohibited and punishable by applicable County disciplinary procedures, which may include termination and/or criminal prosecution depending upon the nature and severity of the transgression. The term public resource as used in these procedures include not only the unauthorized use of equipment, hardware, software or tangible articles, but also the employee time expended in the engagement of the unauthorized use while on County time.

Examples of unauthorized use of software may include streaming music, stock tickers, news reels, movie downloads, games, screensavers used from the Internet, unauthorized messaging software such as AOL, YAHOO, Windows Messenger; and “chat” software. Authorized or unauthorized use of software may also be defined at the discretion of County management.
Employees may not:
1. Use technology resources for personal gain, or to support or advocate for non-County related business or political purposes.
2. Create, distribute, upload or download any disruptive, abusive, harassing, threatening, or offensive messages, including offensive comments or graphics about sex, race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
3. Use technology resources for illegal or unlawful purposes or to support or assist such purposes.
4. Use technology resources for wagering, betting or selling chances or to support or assist such purposes.
5. Use technology resources for personal long distance telephone calls.
6. Attempt to circumvent or subvert system or network security measures, provide internal network access to any non-Users or use your account to gain unauthorized access to external networks and systems.
7. Mount an attack on the security of any system (i.e. attempting to hack or introduce viruses into a system).
8. Use the network to disrupt network Users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer "worms" and viruses, and sustained high volume network traffic that substantially hinders others in their use of the network.
9. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
10. Install or use encryption software on any Charleston County computers without first obtaining written permission from your Department Head and Technology Services. Users may not use encryption keys or encryption passwords that are unknown to their Department Head.
11. Engage in online fundraising (unless approved by County Administrator; e.g., United Way)
12. Engage in mass-mailing or send County-wide messages without department head, PIO, DCA or County Administrator approval.
13. Send County-wide mailings about viruses, or other warnings about outside computer attacks (these are almost always a hoax, and should be turned over to Technology Services for disposition).
14. Initiate or forward chain letters by email.
15. Spoof (disguise) your identity or send anonymous e-mails or send e-mail under another employee’s name without permission.
16. Download any non-standard or non-business related files or software, including "freeware" and/or "shareware" programs unless previously approved.
17. Load personal Internet Service Provider accounts (i.e. AOL, CompuServe, etc.) on County owned equipment.
18. Unless expressly authorized, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the county is strictly prohibited. Unauthorized disseminating of this information may result in substantial civil liability as well as severe criminal penalties under the Economic Espionage Act of 1996. Employees must obtain permission from their Department Head to gain access to the County’s Internet facility.
19. Make or use illegal copies of copyrighted software or other mediums, store such copies on County systems, or transmit them over the County network.

It is the responsibility of the supervisor, manager and/or department head to be aware of how the County’s Internet facility is being utilized by his/her employees and ensure that employees are periodically informed and aware of the technology procedures at a minimum on an annual basis.
1. Identify those employees under their cognizance they desire to grant Internet access. The Department Head must sign the Internet access request. No delegation of this responsibility will be permitted.
2. Cognizance of how the County’s Internet facility is being utilized by employees.
3. Ensure that employees are periodically informed and aware of the policies associated with the use of the Internet at a minimum on an annual basis.
4. Review usage reports provided by Data Processing for impropriety and/or abuses.

6.3 Network Monitoring
All computer applications, programs, data and work-related information created or stored by County employees on County information systems and resources are the property of Charleston County. Charleston County employees shall have no expectation of privacy in anything they store, send or receive on the County’s computer systems. Charleston County may monitor messages or data without prior notice. Charleston County is not obligated to monitor e-mail messages. The County reserves the right to
access and monitor e-mail use and any other computer related transmissions, as well as stored information, created or received by County Users with County technology systems and resources under the following circumstances:

1. Performance monitoring or problem solving purposes
2. Necessary in the course of an investigation for possible violation of County policies
3. There is reasonable suspicion that a User has committed, or is committing a crime against the County or for which the County could be liable
4. Random or automated monitoring to ensure that content is in compliance with the business’s established policies.
5. Request for monitoring is made by appropriate authority
6. Required to do so by law

The reservation of this right is to ensure that public resources are not being wasted and to ensure the County’s information systems are operating as efficiently as possible in order to protect the public’s interests. This includes blocking access to certain Web sites for which access is deemed to be in conflict with County policy.

6.4 E-Mail Records Retention

E-mails and attached documents are the property of the County, and the citizens of Charleston County, and are subject to County records management policy. Generally speaking, e-mail messages represent temporary communications that are non-vital and may be discarded routinely. As a result, the e-mail system should not be used to transmit sensitive materials (for example, personnel matters) that may more appropriately be communicated by written memoranda or personal conversation.

However, depending on the content of the e-mail message, it may be considered a more formal record and need to be retained pursuant to a department’s record retention schedule. Examples of this include policy, decision-making, connected to specific case files, contract related or otherwise an essential part of a larger record, or other memorandum of significant public business.

Users are cautioned that deleting an e-mail message from a User’s own mailbox does not mean all copies of the message are also deleted. The message may still reside in the recipient’s mailbox, may have been saved in some other folder, or forwarded to other recipients. Also, any message sent the day before may be saved in the nightly system backup and retained for a period of time.

The County has established a procedure that e-mail messages will be retained on the County’s e-mail server for no longer than 30 days, and then deleted. PC Users may archive their e-mail to their local hard drive for retention. Network Users may download e-mail to their network “home” drive (H:) for retention. All messages will be deleted from User “trash” folders after 7 days.

As with other records, no e-mail record may be destroyed after it is requested for reasons including but not limited to: employee termination & disciplinary action, until: a) the request is granted, or b) 60 days have elapsed after the request is denied or c) litigation on the records availability is complete and any court order has been obeyed.

Managers and supervisors may, with Department Head approval, access, as necessary, an employee’s e-mail if employees are on leave of absence, extended leave, or are transferred from one department to another.

7 Security

Charleston County has a comprehensive computing environment that encompasses a broad array of networking, mainframe, server and desktop computing platforms as well as the complimentary systems software. Users should never consider electronic communications to be either private or secure. E-mail and data could potentially be stored indefinitely on any number of computers, in addition to that of the recipient. Copies of e-mail messages or altered messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect user names may be delivered to persons that the sender never intended.

Each User is responsible for ensuring that his or her use of outside computer and networks, such as the Internet, does not compromise the security of Charleston County’s computer network. This duty includes taking reasonable precautions to prevent others from accessing the County’s network without authorization and to prevent introduction and spread of viruses.

7.1 Network / Internet Security

Standards and requirements exist to ensure security and availability of the data and systems. The County’s network connects to the Internet through a firewall.
The County follows a three-tiered structure for web-enabled systems that are accessible from the Internet. These systems will host their web pages on a web server while the application and databases will reside on different server(s). This configuration promotes maintainability and is desired on all new systems being evaluated for the County. This also allows the web server to be placed in a safe zone, (referred to as the “DMZ” – Demilitarized zone) with the application and database servers on the internal network for enhanced security. Under no condition is access allowed directly from the Internet to the internal network.

A server in the DMZ may establish a point-to-point connection to an Application on the internal network if required to perform an approved function. Any DMZ server required to communicate with a database server in the internal network should do so through a proxy configured for a non-standard port. These ports are well documented (www.iana.org) and are subject to extensive hacking.

Under no circumstances will a server on the DMZ have the ability to initiate a conversation with a workstation on the internal network. Also DMZ servers are not allowed to connect out to the Internet via HTTP protocol. In addition, all web servers should have their systems configured to disable all non-essential functionalities (SMTP, SNMP, FTP). FTP or any other access is provided only if required for an approved function and does not compromise the security of the County’s Computing Environment.

Security Patches - The County has a process to update all servers with the latest security patches to enhance security. The application vendors should adhere to the industry practice of compliance to the latest version of system software levels to ensure maximum security to information and services provided by the County.

Network Devices – Prior approval from Technology Services must be obtained before any of the following activities are attempted. These are not allowed by default:
* Connecting any networking devices to the County network.
* Usage of modems on individual servers / desktops / workstations for remote access purposes.
* Allowing non-county agencies or entities to access the County network without prior Technology Services approval.

The following activities should only be carried out by Technology Services or its authorized designees:
* Connecting networking devices to the County network.
* Interconnecting external networks by routers.

To maintain the security of the County network, all the Virtual Private Network (VPN) Users should ensure that:
* Their PCs have the most current virus protection installed
* Operating system has all the recommended patches installed
* Browsers have all the recommended patches installed.

7.2 Anti-Virus Protection

The County network is protected from viruses with the help of firewalls, e-mail scanning software and desktop scanning software. However, Users must follow these guidelines:

In some cases, simply reading an e-mail can spread a virus to a User’s computer, and from there to many other internal and external County recipients. The County will take prudent measures to scan incoming e-mail and attempt to intercept viruses. However, no safeguard is foolproof, and viruses can find their way into County Users’ computers from a variety of other ways (e.g., diskettes from other computers, internet file transfer, etc.). Each User is responsible for taking reasonable precautions to avoid introducing viruses into the County network, including but not limited to:
* Always run the County standard, supported anti-virus software that the County provides.
* NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying your Trash.
* Delete and never forward spam, chain, and other junk e-mail.
* Never download files from unknown or suspicious sources.
* Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
* Always scan a floppy diskette from an external or unknown source for viruses before using it.
* Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Viruses and Laptops

Viruses can gain back door entry via laptops that are normally outside the network and which may get infected. To eliminate such risks, the following guidelines should be used while using laptops on the County network.
1. Always make sure that you have current antivirus protection on the laptops. County provided laptops should have eTrust antivirus software on them. If it is not present, please contact Technology Services Help Desk.

2. If connected on the county network, the antivirus signature for this software is updated daily. All other county laptop Users should ensure that they periodically, (weekly) connect the laptops to the county's network for two continuous hours to get the signature updates. If it is not possible, please contact the Technology Services Help Desk for a change in the laptop settings.

3. Scan your hard disk periodically for any virus. Once a week is an ideal frequency as this would help the ongoing detection of any virus, or new virus, on your machine.

4. Keep your Windows software "patched." Information will be provided by the Help Desk and on the County Intranet to help Users do this. Note that unpatched Windows software is vulnerable to virus attacks.

It is desired that non-County laptops not be connected to the County network. If it is totally unavoidable a user must:

1. Ensure that the laptop has antivirus software loaded on it.
2. The Signature file for the antivirus software is current.
3. The laptop is scanned for viruses just before it is connected on the County's network.

Following these steps while using your laptop will help ensure the safety and security of the County's data and network. For questions, please call the Help Desk or reference the County's Intranet site for more information.

**E-mail Scanning**

In order to provide further protection for all our County Users, Technology Services has implemented additional measures for electronic scanning of incoming e-mail. All e-mail attachments coming to the County will be electronically scanned for key words that are either sexually explicit, have drug culture references or contain known phrases indicative of spam, hoaxes or viruses. Also, the “Subject” line in e-mail will be scanned for the same kinds of key words. Any e-mail with words or phrases matching the key word list will be saved in a quarantine file. If you receive a message that an e-mail or attachment has been rejected, you will have four weeks to contact Technology Services and ask to see the rejected e-mail, in case the scanning process rejected something important to you. Otherwise, the rejected e-mail will be disposed of automatically after four weeks.

It's important to note that email scanning is an electronic comparison to a table of inappropriate words and phrases. This electronic scan will reduce offensive material and make it much more difficult for purveyors of junk e-mail or viruses to interfere with normal operations.

### 7.3 IDs & Passwords

Passwords are an important aspect of computer security. They are the front line of protection for User accounts. A poorly chosen password may result in the compromise of Charleston County's entire corporate network. The scope of these procedures include all personnel, including third parties, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Charleston County facility, has access to the Charleston County network, or stores any non-public Charleston County information. As such, all are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Users are responsible for safeguarding their passwords for access to the computer system. Users are responsible for all transactions made using their passwords. No User may access the computer system using another User’s password or account without express permission or portray oneself as another User. In order to provide appropriate network security, these procedures mandate that County Technology Services utilize passwords and periodically require Users to select a new password, one that they have not used before. Although Users have confidential passwords, this should not be construed to mean that the application data is the property right of the User or that network, internet nor that e-mail access is for personal confidential communications or that the password is to protect the employee’s privacy. Users are expected to follow these guidelines:

* Passwords shall remain confidential and should not be printed, stored online or given to others.
* Passwords shall be changed every 90 days.
* Passwords shall be at least six characters long.
* Passwords shall contain characters from at least three of the following four classes: (i) English upper case letters, A, B, (ii) English lower case letters, a, b, (iii) Westernized Arabic numerals, 0,1,2, and (iv) Non-alphanumeric (“special characters”) such as punctuation symbols.
003 Charleston County, SC – Technology Usage Procedures

* Passwords may not contain your User name or any part of your full name.
* Passwords must not be inserted into e-mail messages or other forms of electronic communication.
* The password shall not be a word found in a dictionary (English or foreign)
* The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters,
* The password shall not be a computer term, name, command or a site, company, hardware, or software name.
* The password shall not be your birthday or other personal information such as address and phone number.
* The password shall not be a word or number pattern like aaabbb, qwerty, zyxvwuts, 123321, etc.
* The password shall not be any of the above spelled backwards.
* The password shall not be any of the above preceded or followed by a character (e.g., secret!, Isecret).

7.4 Third-Party Access
Charleston County has a Third-Party Access procedure which establishes the rules and responsibilities for:
1. Charleston County employees who are responsible for the contracting and/or supervising of the third party and
2. third-party access to Charleston County information systems and the data center.
A third-party is any individual from an outside source (contracted or otherwise) who is granted access to County information systems. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.
The procedure addresses access to the data center and to our information systems. Contractors or other third parties who violate these procedures may have their contract revoked. Other legal remedies, including criminal prosecution, may also be pursued.

7.5 Desktop Security
Please follow the guidelines below to avoid security breaches:
* Close sensitive or confidential applications and turn off your monitor when you leave your desk.
* Do not leave portable media such as CDs or floppy disks in drives.
* Turn off your computer when you leave for extended periods.
* Never write your passwords on a sticky note nor try to hide them anywhere in your office.
* Remove printouts from printers before leaving your office.
* Shred sensitive printouts or paper when you are done with them.
* Where appropriate:
  o Use a screen filter to minimize the viewing angle on a computer monitor.
  o Enable a password-protected screen saver. (Must be disabled for technical support.)
  o Clear cache files on computer and memory on devices like printers regularly.

7.6 Modem Use Procedures
The County of Charleston has spent considerable money and effort to secure the network. A network modem bank is installed for modem usage by employees connected to the network. Modern communication is allowed only to transact County business. It is the objective of Charleston County to balance the County's need for network security and the employee's need for modem communications, prevent outside computer hackers and viruses from destroying computer data both on the network and on PC's and to prevent unauthorized access into County computers and data files.
The County will allow external modems attached to a PC (connected to the County network) only in the case where communication software needed to transact county business will NOT run on a network modem bank and other similar communication software is not available. The authority to allow external modems rests with Technology Services. It is the responsibility of the employee to log off the network when using this modem and power off the modem when not in use.

7.7 Portable Memory
The use of USB flash drives, small, keychain-sized storage devices or other portable memory is discouraged and requires Technology Services approval.

7.8 Computer Data Backup
For all servers in the county's data center in the Public Services Building, the following backup procedure is administered:
* Daily – Monday through Thursday – Incremental backups, with two-week retention period
* Weekly – Friday/Saturday – Full backups, four-week retention period
Monthly – Last Friday of every month – Full backups, 12-month retention period
Hurricane evacuation takes the last full backup of our systems, or last Friday's backup, or the last monthly backup offsite.

Full Backup: Every Friday each server is fully backed up. This includes the system files, application files and data files. When Friday falls on a holiday, the preceding working day will be treated as Friday for backup purposes. If there is a failure on a Monday morning, we just need these backup tapes to be able to restore.

Differential Backup: Backup that copies all the files and folders that have changed since the last full backup to a backup media (tape). Monday's backup would include all files and folders that have changed since last Friday. Tuesday's backup would include all files and folders that have changed since last Friday, and so on. If we have a failure on a Thursday morning, we would just need the Friday's full backup tapes and the Wednesday's daily backup tapes to be able to restore the data.

For every workday other than Friday, the differential backup is taken for system, application and data files. The same set of tapes may be used for a complete week depending on the data that gets backed up during the week. However, for all open systems, the backup process has been refined so that differential backups taken on Mondays and Wednesdays go on one set of tapes, and those taken on Tuesdays and Thursdays go on a different set of tapes. This ensures that if a corruption of a single tape occurs, we still have a good copy of previous day’s backup.

Monthly Backup: Backup of the last Friday of each month is treated as a monthly backup.

Retention Schedule: Differential backups are retained for two weeks and weekly full backups are retained for a four-week duration. The tapes are overwritten after four full weeks. The monthly backup is retained for 12 months (14 in special cases) before the tapes are reused.

Offsite Storage: After holding the backup tapes in the Public Services Building for 10 days, (three days in the data center, one week at another location across a firewall in the Public Services Building), it is sent to the Record Center for offsite storage until the tapes are recycled. To address the distance concerns due to the close proximity of the Records Center to the Public Services Building, Technology Services has a backup data storage unit at the County Office Building which houses a nightly incremental backup of a subset of “critical” data. Once all critical systems are moved off of the mainframe, or the mainframe is replaced with components that allow for remote data storage, the remainder of the critical data can be stored in the back storage unit downtown.

EMS has a backup server in the Radio Prime Site Building outside of the Public Services Building at the base of the radio tower. The EMS backup server is also intended to be used as a mobile server and enables EMS to quickly gather it along with other equipment there to move to the mobile dispatch center. EMS data is backed up by EMS staff and is kept in three separate systems - tape backups, network attached storage unit, and replicated in real time to the backup server in the radio prime site building. EMS is working with Technology Services to place their backup tapes with ours in order to store them at the Records Center and to be taken inland if threatened by a hurricane.

Exceptions: Based on the critical nature of the data and complexity of the application, certain databases follow different backup schedules:

* Bi-Tech (Financial and Human Resources System), CAMA (Computer Aided Mass Appraisal System): Daily full database backup.
* GIS Orthophoto Database: Since this is static data, we perform monthly full database backup and after a major change to the database.

7.9 Security Access Removal

Physical Security: For employees who have left the County, changed roles, or access needs have changed, the department head or authorized designee should submit the Badge/ID Request form immediately to HR. This form can be found on the County Intranet site.

Computer System Security: Removal is one of several items on the “Employee Check Out List” which is used when an employee leaves the County. The Department Head or authorized designee must fill out a “Technology Security Request Form”, and a “Bitech Security Request Form”, if applicable, located on the County Intranet site and submit to Technology Services immediately upon employee departure or separation of employment. The “Technology Security Request Form” should reflect all systems for which a terminated employee had access. Please note if e-mail or file data is to be transferred to the Department Head’s account or other location. Otherwise, any and all data associated with the account will be deleted.
Persons no longer employed have no right to the contents of their e-mail messages or data stored in County systems, and should not be allowed access to the internal system.

8 Weather Emergencies and Protection of Computer Equipment

Upon activation of the Emergency Operations Center (EOC) for weather emergencies the following steps are to be taken by each User to help protect both computer hardware and software.

* Backups should be taken of all personal computers that are not attached to the network. Both backup disk(s) and application software are to be stored in a dry and secure location for safekeeping. If the personal computer is attached to the network and the data files reside in a network directory, it is not necessary to create backups, as these files will be backed up for you. If you are attached to the network but keep data files on your hard drive, you should copy those data files (i.e. word processing documents, spreadsheets, databases, etc.) to a network directory so it may be backed up for safekeeping. Please note that every individual has quota of 20 MB on network drive.

* All computer equipment should be powered off. This applies to personal computers; workstations, printers and any associated peripheral devices (i.e., tape backup units, modems, scanners, etc.). After powering down the equipment, disconnect the power cables from the receptacles to protect equipment from potential surges from lightning.

* Any equipment located on the floor should be moved to a higher location and away from any windows.

* All monitors should be turned so that no screens face the direction of any windows.

* Cover all equipment with plastic sheeting/bags and secure with masking tape. The purchasing of plastic bags and/or masking tape is the responsibility of the individual departments.

Operations during an emergency are outlined in a separate plan prepared by Technology Services and shared with relevant departments.

9 Procedure Infraction

County employees who violate these procedures may have their access removed and may be subject to disciplinary action up to and possibly including termination. In addition, contractors or other third parties who violate these procedures may have their contract revoked. Other legal remedies, including criminal prosecution, may also be pursued if warranted.

It is the procedure of Charleston County to handle infractions as follows:

1. The violation should be reported to the User’s supervisor or manager.

2. The User’s supervisor should approach the violator(s) directly with the findings, ensure the User is aware of the procedure, and give them the opportunity to cease and desist; or, depending on the severity, follow disciplinary procedures consistent with the guidelines and policies of “Charleston County Personnel Policies and Procedures.”

10 Computer Support / Technology Requests

10.1 Help Desk

Technology Services offers support for existing County computer systems by calling a local number during business hours, 8:30 am-5:00 pm, Monday through Friday. For those departments that require 24/7 support, (EMS, Sheriff and Emergency Services), cell phone and pager numbers have been provided. You may also enter any non-urgent requests via the Help Desk link on the County Intranet Site. Help Desk personnel will attempt to resolve problems via the telephone or via remote control, where feasible, and where the User gives express permission for remote control support.

Technology Services discourages calling specific technical resources as those resources may be unavailable. Using the Help Desk for support ensures a timely response by the appropriate resource, documentation for tracking of problems and data to pinpoint where resources might be concentrated in order to resolve ongoing problems.

10.2 Authorization for Technology Services requests

Department Heads can authorize others on staff to submit Technology Services requests and security access changes for County Technology Systems. An “Authorized Signatures for Technology Services” form is available on the County Intranet site for this purpose.

10.3 Technology Services requests

Currently Charleston County provides forms for which you can download and fill out or online access to non-emergency Service Requests on the County intranet site for the following types of requests to Technology Services:

* Work Order Requests – work requests for the application development team to enhance or add functionality to current applications or to create new applications. Examples of this type of request would
be to add a new function to our Court system, create a Cobra/Retirement database or add a permit request form to the County's Internet site. Authorized signature is required.

* Service Requests – Used for non-emergency work requests for the infrastructure, network or desktop staff. This work typically is for a PC move, software upgrade or to connect a printer to the network. A downloadable form exists for this purpose, or a form which can be submitted online.

* Hardware / Software Requests – requests to purchase new hardware or software. This request may include software, printers or other devices. Authorized signature is required.

* Security Requests – requests to add, change or delete a User’s access to specific Charleston County applications or systems. Authorized signature is required.

* BiTech Security Requests – requests to add, change or delete a User’s BiTech system access.

* Audio Visual/Video (AV) Requests – request for AV equipment setup for a meeting or presentation at the Public Services Building. 48 hours advance notice is desired. Requests are automatically sent to the appropriate resources when submitted online.

* Copier Network Installation Request – requests to connect a network-able copier to the County network.

* Computer Equipment Relocation Requests – used when a piece of computer equipment is relocated from one department to another or location within a department. The information requested is used to update the Technology Services inventory and asset database.

* Production Control Request – Requests for non-automated mainframe jobs to be run.

11 Computer Training
Charleston County contracts with PST, Inc. to provide training courses for the desktop software programs most used by employees. All Users are encouraged to invest the time to attend training, as this will enable Users to be more productive with the software tools provided by Charleston County and reduce support costs. Most classes are conducted in the Technology Training Room, Room C320 of the Public Services Building. A link to the training calendar is located on the County Intranet site. Choose your course, obtain appropriate approval, then click on the "Register for Course" option. From this option, you will be linked to the County's registration site where you can sign up for the course and select from other available services. You can also register by phone by calling PST directly at (843) 529-0098.

12 Definitions

* Attachments - Files created in other applications (such as Word, Excel).

* E-Mail - An electronically transmitted message, along with any attachments and any information appended by the e-mail system.

* E-Mai System - Computer hardware and software system that allows personal computer users to send, receive and store messages, documents and files with other individuals or groups of people over an internal network or the Internet.

* Encryption - A means of coding messages so they appear to be random characters. Encryption has two benefits. First, it prevents disclosure of sensitive information to unauthorized third parties. Second, encryption allows for "authentication" of the information sent.

* Freeware - programming that is offered at no cost, which is copyrighted so that one can't incorporate its programming into anything one may be developing.

* Hacking – the unauthorized attempt or entry into any other computer or system.

* Internet – a world wide computer network through which you can send a letter, chat to people electronically or search for information on almost any subject you care to think of. Quite simply it is a "network of computer networks".

* Internet Browser - an application that displays HTML and other information found on the Internet. Netscape Communicator, Internet Explorer, and Mosaic are examples of browsers. This type of client software accesses the World Wide Web and Gopher services and lets you drift from link to link without having to have a purposeful search.

* Internet Service Provider (ISP) - an entity that charges startup and monthly fees to users and provides them with the initial host connection to the rest of the Internet usually via a dialup connection.

* Technology Services - Technology Services Departmental label referring to the employees of Charleston County and current outsourced information technology vendor staff.

* Public Record – as defined in South Carolina Freedom of Information Act (FOIA).

* Public Resource - Includes not only County equipment, hardware, software or tangible articles, but also the employee's time expended while on duty with the County.

* Risk - Those factors that could affect confidentiality, availability, and integrity of Charleston County's key information assets and systems. Charleston County is responsible for ensuring the integrity,
confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

* Shareware - software that is distributed free on a "trial basis" with the understanding that the user may need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date (after 30 days, the user can no longer get access to the program). Other shareware (sometimes called liteware) is offered with certain capabilities disabled as an enticement to buy the complete version of the program.

* Third Party – Any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

* Trade Secret – as defined by law.

* World Wide Web (WWW) - a hypertext-based distributed information system for linking databases, servers, and pages of information available across the Internet.

13 Signature of Agreement

I, ___________________________________________ have read and agree to abide by the Technology Usage Procedures while employed, affiliated with, or doing business with Charleston County.
004 Martin County, FL – E-mail Acceptable Use Policy

E-mail Acceptable Use Policy
PURPOSE
1.0 - Purpose
Electronic Mail (E-mail) access provided to Martin County employees is intended to facilitate County business objectives for employees and other business associates for communications, collaboration, research and/or other work related tasks. The utilization of E-mail can enhance the productivity of the Martin County work force. The goal of this policy is to maximize and ensure proper use of this resource.

2.0 - Overview
Martin County's Electronic Mail System provides employees with nearly instantaneous electronic communication capabilities. This connectivity with local, regional, national and worldwide interests promotes staff collaboration and informed decision making. Effective utilization of E-mail reduces the traditional but non productive reliance on paper based communications for these purposes and promotes innovation in the delivery of services to the citizens of Martin County.

3.0 - Policy
3.1) All Martin County data processing and communications systems, including the E-mail system, are Martin County property and are intended for County business use only.
3.2) The Martin County E-mail system must not be used for employee personal reasons or personal gain, to access, support or advocate non County related business or for any other non business purposes.
3.3) All Martin County E-mail data, including materials created, received or transmitted within the system are the property of Martin County.
3.4) The County through its managers and supervisors will review the contents of any employee's E-mail activity whenever necessary for County business purposes. However, employees may not intentionally intercept, eavesdrop, record, read, alter or receive other persons' E-mail messages without proper authorization.
3.5) E-mail messages may need to be retained and/or made available for inspection as public records depending on their content. If so, the Department of State Records retention schedules shall apply. (See: Retention of Non-Transitory E-mail messages, below).
3.6) Employees who misuse E-mail privileges shall be subject to progressive discipline up to and including discharge.
3.7) Employees, contractors, part-time employees, volunteers, and other individuals who are provided access to Martin County's E-mail system should keep in mind that they represent the County and must conduct themselves appropriately at all times.
3.8) Remember that your personal comments and opinions may not reflect Martin County policy, therefore the following disclaimer should be attached to all E-mail signature files for messages sent to external destinations:
"The comments and opinions expressed herein are those of the author of this message and may not reflect the policies of the Martin County Board of County Commissioners."
3.9) Department directors are responsible for the implementation and adherence of this policy within their departments. Department directors (or their designees) are encouraged to work with their departments' entire staff toward that end.
3.10) Each Department director shall provide every staff member, contractor, part-time employee, volunteer, or other individuals who are provided access to Martin County's E-mail system with a copy of this policy. The attached policy acknowledgment form must be signed by the individual and shall be maintained in their Personnel file or in the case of a non employee, wherever designated by the Department director.
3.11) In the event that any department or division policy contradicts this policy, this policy shall govern.
3.12) This policy may be changed only upon the written approval of the County Administrator.

4.0 - Confidentiality
4.1) Although confidential passwords are issued, users should be aware that this does not suggest that the Martin County E-mail system is for personal confidential access or communication, nor does it suggest that access to and use of the Martin County E-mail system is the property right of the employee.
4.2) Since no computer system is completely secure, the E-mail system is not intended to transmit sensitive materials, such as personnel decisions and other similar information which may be more appropriately communicated by written memorandum or personal conversation.

4.3) Users should not share their passwords with anyone else. Others might then use it to gain unauthorized access to the Martin County E-mail system.

4.4) User passwords should be periodically changed to ensure security of the E-mail system.

5.0 - Prohibited Uses
The Martin County E-mail system shall under no circumstances be used to:

1. Solicit, proselytize or participate in commercial ventures, religious or political causes, outside organizations, or any other non County job related solicitation or participation.

2. Create, access or transmit any obscene, disruptive, slanderous, defamatory, derogatory or otherwise offensive or illegal information. Among that which would be considered offensive is information which contain sexual implications, racial slurs, gender specific comments, or any other comment or material that offensively addresses someone’s age, sexual orientation, religious or political beliefs, national origin, or disability.

3. Transmit copies of any document in violation of copyright laws.

4. Transmit material which is specifically exempted from public inspection under Florida Statutes Chapter 119 - Public Records Law. For example, personal information (telephone, address, social security numbers) for law enforcement officers, firefighters, code enforcement officers or Judges.

5. Seek information on, obtain copies of or modify files/data/passwords belonging to other users. Also, users must not represent themselves as other users unless specifically authorized to do so in writing by a Department Director.

6. Compromise the integrity of Martin County or Martin County resources in any way.

6.0 - Applicability

6.1) This Martin County E-mail policy applies to all employees, contractors, part-time employees, volunteers, and other individuals who are provided access to Martin County's E-mail system.

6.2) Third parties should only be provided access to the Martin County E-mail system as necessary for their business purpose with the County, and then only if they agree to abide by all applicable rules.

6.3) Contractors and third-party users who are in violation of this policy may lose their E-mail system privileges and/or have their contracts revoked. Additional legal remedies may also be pursued.

7.0 - Disposition of Transitory E-mail messages
According to the most recent B.A.R.M. General Records Schedule GS1 many E-mail messages are considered "transitory communications" which are non-vital and may be discarded routinely without written approval by the B.A.R.M. The GS1 sets the following retention period for E-mail containing Transitory Messages:

Retain until obsolete, superseded or administrative value is lost. Examples:

a) Routine announcements and information including notices of seminars or workshops, queries regarding processes or ideas and general information regarding programs;

b) Reference files that are general information files used in daily functions of the administrative area;

c) Meeting notices, statistical records, reading files (copies of materials archived elsewhere) and recipients inter-departmental memos.

County employees should be aware that even when they have deleted a message from their mailbox it may not yet have been completely removed from the E-mail system. The message may be residing in the recipient's mailbox or may have been forwarded to other recipients. Furthermore, the message may be stored temporarily on the server's backup system.

A short term automated backup of Martin County E-mail is performed by the Information Services Department as part of standard data processing contingency practices. It is not designed nor intended to comply with the Public Records Law, but to ensure that all data can be restored in the event of a catastrophic occurrence. For this purpose, all E-mail messages transmitted or received are archived for a period of three (3) days during which time they can be restored if needed. After that period, tape media used to archive these messages are overwritten and the messages can no longer be accessed or restored by ITS. Therefore, staff shall plan and implement their own specific procedures, by Department, for the management and accessibility of E-mail in order to ensure compliance with the law. For further guidance, contact Information Technology Services at X4800.

8.0 - Retention of Non-Transitory E-mail messages
E-mail messages are public records whose retention requirements vary by law according to the nature of their content. Florida's Public Records Law creates a significant challenge in managing E-mail, mainly because E-mail message content is often informal and/or transitory in nature. E-mail usage allows County staff to eliminate the handling, filing and archiving tasks associated with paper-based systems. However, it does not eliminate the user’s responsibility to manage records as prescribed by law - regardless of the format of those records. Because E-mail and paper-based communications are utilized so differently, all users shall develop a separate and specific method for periodically reviewing, storing and/or deleting their E-mail records.

County staff are responsible for adhering to the retention schedules established by the Florida Department of State: Bureau of Archives and Records Management for all public records, including E-mail messages. These schedules are available at the Department of State's web site as follows:
http://www.dos.state.fl.us/dlis/barm/genschedules/gensched.htm

Keep in mind that these retention schedules are based on a record's informational content, not its format. County agencies are required to file records disposition requests via ITS Records Management for any Public Records which have met their recommended retention periods and are to be destroyed, including any Non-Transitory E-mail messages which may fall under that category.

Depending on the content of an E-mail message, it may be considered a formal record and should be retained according to the B.A.R.M. record retention schedules. Examples of records which would be considered Non-Transitory: General correspondence, senders interdepartmental memos, and most fiscal and budget records. Any other record that sets policy, establishes guidelines or procedures, certifies a transaction or becomes a receipt would also be included in this category and must be retained for the applicable retention period according to the relevant Records Schedule.

E-mail which falls into the category of "retain until administrative purpose is served" may be deleted when no longer needed. However, E-mail which has a longer retention period, such as correspondence or senders memos, must be retained through its applicable retention period according to Departmental procedure. Like all Public Records, it must remain easily accessible during its retention period. For further guidance, contact Information Technology Services at X4800.

9.0 - Bulletin Board, Listserv and Conference participation
Bulletin board or listserv type systems which are available via E-mail allow multiple users to access and exchange information with other users who are provided access to that bulletin board or listserv. These systems may be set up to limit access to specific individuals. Most messages on a bulletin board / listserv type system are accessible to many users or posted for public dissemination. All Martin County E-mail Bulletin Board / listserv and conference participation must be for County business purposes only.

10.0 - Applicability to Employees, Part-time Employees, Contractors, and Other Users
10.1) This E-mail policy applies to all employees, contractors, part-time employees, volunteers, and other individuals who are provided access to Martin County's E-mail system.
10.2) Third parties should only be provided access to the Martin County E-mail system as necessary for their business purpose with the County, and then only if they agree to abide by all applicable rules.
10.3) Contractors and third-party users who are in violation of this policy may lose their E-mail system privileges and/or have their contracts revoked. In addition, other legal remedies may be pursued.

11.0 - Management & Employee access rights
11.1) Martin County Supervisors or management may access an employee's E-mail files if employees are on leave of absence, vacation, are transferred from one department to another department or whenever they deem necessary for the County's business purposes.
11.2) Former County employees have no special access rights to their E-mail messages other than a public records request for records within their retention period.

12.0 - Laws & Penalties
12.1) All users of the Martin County E-mail system are subject to the Martin County Disciplinary Code, Personnel Manual and applicable Collective Bargaining agreements, as well as all State and Federal Laws.
12.2) The misuse of E-mail privileges shall subject the offender to progressive discipline up to and including discharge. In addition, violations of this policy or misuse of the Martin County E-mail system may be referred for criminal prosecution.

E-mail Acceptable Use Policy User acknowledgment
I have read and hereby acknowledge and accept the terms of the Martin County E-mail Acceptable Use Policy and agree to abide by its conditions as written whenever using the Martin County E-mail system.
General Computing Resource Usage Policy

PURPOSE
Computing resources provided to Martin County employees are intended to facilitate County business objectives for employees and other business associates for communications, research, development of work-related deliverables and/or other work-related tasks. The utilization of computing resources can enhance the efficiency and effectiveness of the Martin County work force. The goal of this policy is to ensure the proper use of this important resource by outlining its acceptable use, as well as defining certain prohibited uses.

As used in this policy, the term “Computing Resources” includes but is not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, all of which are the property of Martin County. These systems are to be used for business purposes in serving the interests of the County, and of our citizens and customers in the course of normal operations. This policy is in place to protect the County, its employees, and other business associates from risks caused by inappropriate use including virus attacks, compromise of network systems and services. Effective security is a team effort involving the participation and support of every Martin County employee and affiliate who deals with information and/or information systems. Every computer user is responsible for understanding this policy and for conducting their activities accordingly, and they will be held accountable for actions relating to this policy.

1.1 General Use and Ownership
1.1.1 Employees should be aware that the data they create on County systems remains the property of Martin County.
1.1.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of computer systems. In the absence of such guidelines, section 1.11 of this policy, "Personal Use of County-Owned Computer Systems," shall apply.
1.1.4 For security and network maintenance purposes, authorized individuals within Martin County may monitor equipment, systems and network traffic at any time.
1.1.5 Martin County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.2 Security and Proprietary Information
1.2.1 Passwords shall be maintained in accordance with the County's Computer Password Policy. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
1.2.2 All PCs, laptops, and workstations should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
1.2.4 Postings by employees from a Martin County email address to newsgroups must contain a disclaimer stating that the opinions expressed are strictly those of the employee and not necessarily those of Martin County, unless posting is in the course of business duties as stated in the County's E-Mail Acceptable Use Policy.
1.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders since they may contain viruses, e-mail bombs, or Trojan horse code.

1.3 Unacceptable Use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Martin County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Martin County-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.
1.3.1 System and Network Activities
The following activities are strictly prohibited, with no exceptions:
1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Martin County.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Martin County or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate manager should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others, including family and other household members when work is being done at home.
6. Using a Martin County computing resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policy in accordance with the Martin County Human Resource Policy Manual.
7. Making fraudulent offers of products, items, or services originating from any Martin County account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the individual is not an intended recipient or logging into a server or account that the individual is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification is made to ITS.
10. Executing any form of network monitoring which will intercept data not intended for the individual, unless this activity is a part of the employee's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any other individual or group of individuals (for example, denial of service attack).
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
14. Providing information about, or lists of, Martin County employees to parties outside Martin County.

1.3.2 Email and Communications Activities
1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Martin County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Martin County or connected via Martin County's network.
7. Posting the same or similar non-business-related messages to Usenet newsgroups (newsgroup spam).
8. Any other e-mail usage prohibited by the County's E-Mail Acceptable Use Policy.

1.4 Assignment of Computer Hardware
1.4.1 Martin County determines the computer system needs of employees and how those needs will be met. The County reserves authority to establish and enforce procedures and rules for employee use of County-owned computer systems, software, and data.
1.4.2 The County will assign appropriate computer hardware to a position to enable tasks corresponding to the position to be accomplished.
1.4.3 County-owned desktop computer equipment is the responsibility of ITS. As Countywide property, desktop computers cannot be taken home, relocated or reassigned without prior approval of ITS.

1.5 Assignment of Computer Software
1.5.1 The County will attempt to assign appropriate computer software to a position to enable the tasks corresponding to that position to be accomplished. Contact ITS to request additional software.
1.5.2 Only County-owned software is to be installed on County-owned computers. Exceptions must be approved in advance and in writing by ITS.

1.6 Data and Information
1.6.1 Data, information, or reports produced using County-owned equipment are the property of the County.
1.6.2 Use of County-owned data, information, or reports, are subject to procedures and rules established by the County.
1.6.3 Individuals accessing confidential data are required to maintain the confidentiality of the data.
1.6.4 Individuals originating or updating data must be diligent in maintaining the accuracy of that data.
1.6.5 County-owned data, information, or reports are to be used or copied by an employee only for functions directly related to the employee’s work assignment.
1.6.6 Use of access rights by someone other than the employee(s) to which the rights are assigned is prohibited.
1.6.7 ITS highly recommends saving all data to network/shared drives.

1.7 Account Use
1.7.1 The Information Technology Services department (ITS) has final authority to determine unique account names.
1.7.2 Users are responsible for maintaining the security of their assigned Martin County accounts and files.
1.7.2.1 Authorized users are not allowed to share their accounts with others. The authorized user of the account is responsible for all activities associated with the account.
1.7.2.2 Passwords should be set and changed in accordance with the Computer Password Policy. Passwords should not be revealed to others.
1.7.2.3 In general, ITS does not have access to user passwords.
1.7.3 Users may not use a Martin County account to represent anyone other than himself or herself. Users may not use a Martin County account that they do not have authority to use.
1.7.4 All users are responsible for not wasting network, server or other disk space with unnecessary files.
1.7.5 Accounts on any County-owned computer are limited to employees and other authorized current users such as consultants, contractors and temporary staff. Accounts may be deleted when employment is terminated, when the contract/project expires, or at Martin County discretion. Martin County is under no obligation to recover or protect user files from deleted accounts.

1.8 Software Use
1.8.1 Everyone must follow the copyright laws, trademark standards, software license agreements, and patent information governing software they use.
1.8.1.1 Copying licensed software is generally illegal.
1.8.1.2 The County will support copying exceptions only when authorized in writing by the software publisher.
1.8.2 To determine the copyright policies for County-owned software, employees should contact the Help Desk.

1.9 Network Use
1.9.1 Access to the Internet and the County network is managed by ITS.
1.9.2 Any transmission of data over the Martin County network (e-mail, Internet files and web pages, printer files, etc.) is governed by these guidelines.
1.9.3 Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:
1.9.3.1 Copyrighted material
1.9.3.2 Material protected by trade secrets
1.9.3.3 Illegal activities
1.9.4 Transmission of non-Martin County work-related data is prohibited. Exceptions may be authorized with approval from ITS. This includes but is not limited to:
1.9.4.1 Product advertising
1.9.4.2 Political lobbying or religious material
1.9.4.3 Promoting a personal business
1.9.4.4 For-profit work (e.g., home business, tax preparations, documents generated for a fee)
1.9.4.5 Promoting external organizations
1.9.5 Content and activity of transmissions on the County network is not private. County technicians and system managers may monitor activity on the network as a result of their duties.
1.9.6 Martin County may monitor the content of information transmitted over the Martin County network to investigate complaints of possible inappropriate use. In the course of investigating complaints, Martin County staff will safeguard the privacy of all parties and will themselves follow the guidelines given in this policy.

1.10 Use Of Non-County-Owned Computing Resources
1.10.1 The use of computer resources not owned by Martin County is generally prohibited within the County's IT environment.
1.10.2 Recognizing that there may be legitimate business purposes for the use of non-Martin County-owned equipment within the County IT environment, e.g., consultant-owned equipment, diagnostic equipment, etc., exceptions to this policy may be permitted on a case-by-case basis.
1.10.3 Exceptions to this policy must be approved in advance and in writing by ITS prior to the use of such equipment.

1.11 Personal Use of County-Owned Computer Systems
1.11.1 County-owned computer systems assigned to employee positions are to be used predominately to accomplish the tasks assigned to that position.
1.11.2 County-owned computer systems available to non-employees are provided to support work assignments. E-mail is intended to be used for County-related communication. Internet access is intended to support the County-related business activities.
1.11.3 Incidental use of County-owned computer systems for personal purposes is permitted if:
   1.11.3.1 Use occurs outside of the employee's work schedule
   1.11.3.2 Use does not interfere with work being performed by another employee
   1.11.3.3 Use is not for pay or profit
   1.11.3.4 Use does not consume excessive supplies
   1.11.3.5 Use does not violate software licensing agreements.
1.11.4 Playing computer games is strictly prohibited.

1.12 Laptops
1.12.1 All users of laptops will be permitted to make certain changes to their configuration, such as adding printers, due to the portability of the laptop.
1.12.2 Laptop users in Administration and Commission are exempt from certain software installation restrictions described in this policy.

1.13 Personal Digital Assistants (PDA's)
1.13.1 Due to the large variety of PDA's and the associated operating systems, ITS is recommending that users select devices that run the Palm OS (Palm III, V, Handspring Visor) or the Windows Pocket PC OS (Compaq iPaq). These devices are easy to use, affordable, and meet the needs of the majority of user.
1.13.2 The integrity of the data on PDA's is the sole responsibility of the user. Backup and restoration of the data is accomplished through synchronizing the device with a PC using a docking cradle.
1.13.3 Due to the large number of applications available for these devices, ITS will provide support for the applications that ship with the device as well as the use of Intellisync to synchronize the PDA with Outlook.
1.13.4 Due to limited human resources, the support of PDA's will not be given a high priority at this time.

2.0 Applicability
2.1 This General Computing Usage Policy applies to all employees, contractors, part-time employees, volunteers, and other individuals who are provided access to Martin County computing resources.
2.2 Third parties should only be provided access to Martin County computing resources as necessary for their business purpose with the County, and then only if they agree to abide by all applicable rules.
2.3 Contractors and third-party users who violate this policy may lose all or part of their usage privileges and/or have their contracts revoked. Additional legal remedies may also be pursued.

3.0 Laws and Penalties
3.1 All users of Martin County computing resources are subject to the Martin County Human Resource Policy Manual and applicable Collective Bargaining agreements as well as all State and Federal laws.
3.2 The misuse of computing resources shall subject the offender to progressive disciplinary action up to and including discharge. In addition, violations of this policy may be referred for criminal prosecution.

Intellectual Property Rights:
Materials created and/or produced by users of County-owned resources may be subject to intellectual property rights as established by the County.

MARTIN COUNTY MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESSED OR IMPLIED, FOR THE COMPUTER SERVICES IT PROVIDES.

DEFINITIONS
User - Anyone who holds a valid account on the County's Computer System.
Password - Authorized individual password for access to the County's Computer System resources.
Desktop Computer Equipment
PURPOSE
The purpose of this policy is to clearly identify the role of the Information Technology Services Department with respect to the procurement of desktop computer equipment.

POLICY
Martin County began the Desktop Replacement Program in FY04. The preliminary phase of this Program actually began in FY03 which replaced all Sun Workstations. This Program effectively replaces ¼ of the County desktop hardware (BOCC Desktop Fleet), annually. By implementing a four year replacement schedule, this program ensures that the BOCC Desktop Fleet will not become obsolete and that basic business productivity software can be supported efficiently. Furthermore, employees will gain efficiency as the business software remains standardized. Information Technology Services (ITS) manages the Desktop Replacement Program and maintains a standard hardware/software configuration (referred to as a software image).

**Desktop Computer Equipment:**
The purchase of computers, computer accessories or software must be reviewed and approved by ITS to confirm the purchase adheres to Martin County’s standards. Please note that technology standards are constantly changing, therefore, it is recommended that you contact ITS for the standards, as necessary.

**Laptop as a Desktop:** Desktops provided to Martin County employees are provided with a uniform hardware/software image. Individual users may have a need for a mobile device, such as a laptop or tablet PC. Employees may replace a standard desktop with a laptop during the regular replacement cycle. However, the department is responsible for the difference in cost at the time of purchase and when it reaches the end of its lifecycle, if a laptop is chosen again. In addition, the following criteria must be met:

1. The employee is assigned to work outside of the office and needs access to the county’s computing resources; or
2. The employee telecommutes a minimum of 8 hours per week; or
3. The employee is required to maintain online or computing services while away from their office; or
4. The employee attends meetings away from their office on a regular basis and needs access to the county’s computing resources during the meetings.

**Special Purpose Laptop:** These are defined as laptops that may need to be configured for a specific use or when one is not assigned to an individual. No employee or contractor, etc. may have more than one computer assigned to them. If you have more than one computer assigned to you at the effective date of this policy, ITS will be contacting you to reallocate one of the computers. Some employees may have a laptop that is designated as “special purpose.” Special purpose laptops must meet the following criteria:

1. The software installed on the laptop would interfere with the normal operations of a standard desktop; or
2. The laptop is dedicated to a specific function and the desktop cannot be used for the same function.

**Laptop Pool:** ITS maintains a pool of laptops that may be reserved and checked out for use at conferences, meetings and/or presentations. No other department will maintain a pool of laptops for such purpose. These laptops must be transferred to ITS within 30 days of the effective date of this policy. Generally, laptops that are more than 5 years old will no longer meet current standards. Laptops that are older than 5 years are hereby decommissioned, and shall not be serviced by ITS. Their software and the hardware configuration will not be maintained nor updated by the county. If you need assistance identifying these laptops please contact ITS and/or the Asset Management Specialist in Administrative Services.

**DEFINITIONS**
Desktop: A computer that meets the hardware and software specifications and standards of the Martin County Information Technology Services Department.
Laptop: A laptop computer, usually called a notebook computer by manufacturers, is a battery- or AC-powered personal computer generally smaller than a briefcase that can easily be transported.
computers generally cost more than desktop computers with the same capabilities because they are more difficult to design and manufacture.
PURPOSE
To establish guidelines for all passwords that allow access to computer resources provided by Martin County Information Technology Services.

POLICY
1. General Policy
Martin County Information Technology Services provides access to computer resources including business applications, electronic mail, and the internet. Passwords are assigned for access to these resources to authenticate a user’s identity, to protect network users and to provide security. Information Technology Services creates accounts for users after a valid request is submitted to the service-desk.

2. Confidentiality
Although confidential passwords are issued, users should be aware that this does not suggest that the system is for personal confidential communication, nor does it suggest that access to and use of the Martin County Computer System is the property right of the employee. In order to maintain confidentiality users should not share their passwords with anyone.

3. Passwords
Users are responsible for the security of their accounts. It is the user’s responsibility to use a password that will protect the account from unauthorized use and to change the password as frequently as necessary. If a user discovers that someone has made an unauthorized use of the account they must change the password immediately and the user must also report the incident to Information Technology Services immediately. Users are required to change their passwords at initial login.

Passwords must not contain all or part of the user's account name.

Passwords must be at least six characters in length.

Passwords must contain characters from three of the following four categories:
- English upper case characters (A-Z)
- English lower case characters (a-z)
- Base 10 digits (0-9)
- Nonalphabetic (For example, !$#,%)

Passwords will expire every 365 days. Users may change their passwords at any time. Passwords must differ from previous password.

In order to protect our computer systems at Martin County, Information Technology Services routinely tests users’ passwords for weakness (please see Password Guidelines below). Those users with passwords that are considered weak will be sent an email requesting that the user change the weak password. If a user does not change the password after receiving the weak password notification for 15 consecutive days Information Technology Services will lock the user's account. The user must then contact the service-desk in order to regain access to the account. User accounts will be locked out following 10 repeated invalid password entries in order to make attempts to guess the passwords of users more difficult.

4. Prohibited Uses
Prohibited uses of the Martin County Computer System can be found in the E-Mail Acceptable Use Policy.

5. Applicability
This Computer Password Policy applies to all employees, contractors, part-time employees, volunteers, and other individuals who are provided access to Martin County's Computer System. Violators of this policy may be removed from the computer system and/or have their contract revoked. In addition, other legal remedies may be pursued.

6. Employee Termination and Leave of Absence
Former employees have no special access rights to the computer system other than a public records request for records within their retention period. Employees who are on leave of absence may have their computer privileges suspended until their return to work.

7. Penalties
Failure to adhere to the Computer Password Policy shall subject the offender to discipline up to and including discharge. In addition, violations of this policy or misuse of the computer system may be referred for criminal prosecution. All users of the computer system are subject to the Martin County Disciplinary Code, Human Resource Manual, and applicable Collective Bargaining agreements, as well as all State and Federal Laws.

DEFINITIONS
User - Anyone who holds a valid account on the County's Computer System.
Password - Authorized individual password for access to the County's Computer System resources.

PROCEDURE
Password Guidelines
To minimize password weakness:
* Do not use any part of the account identifier (username, login, etc.).
* Do not use a proper name or any word in the dictionary without altering it in some way. A password is harder to crack if you utilize several of these techniques:
  * Use mixed case.
  * Use random characters.
  * Take the first letter from each word of a phrase.
  * Include at least two digits or punctuation characters.
* Keep your password safe:
  o Do not tell your password to anyone.
  o Do not let anyone observe you entering your password.
  o Do not display your password in your work area or any other highly visible place.
  o Change your password periodically (every 3 months is recommended).
  o Do not reuse old passwords.
Suspected password compromise must be reported to Information Technology Services immediately.
Additional Security Practices:
* Ensure your workstation is reasonably secure in your absence from your office.
* Lock your screen when leaving your work area. Consider logging off the computer or possibly turning off your monitor when you leave your work area.
Records Management Policy and Procedures
It is the intent of this document to communicate to all county staff the procedures and retention criteria for records management and document retention.

POLICY
The attached document, “Martin County Records Management Procedures and Retention Schedule”, provides the official County policy in regards to this matter.

PROCEDURE
The attached policy shall be followed by all staff in order to ensure consistency across the entire organization in the efficient management of County records.

Martin County Records Management Procedures and Retention Schedule
It is the intent of this document to communicate to all county staff the procedures and retention criteria for records management and retention. This policy to be followed by all in order to ensure consistency across the entire organization.

Departments must be aware of the specific retention requirements for each type of document. The State of Florida has created policy to establish the length of time that each document must be retained. This information, a document known as the GS1-L general records schedule, can be found online at:

Please be aware that not all documents require retention.

The Martin County Records Retention schedule is based upon the above mentioned general records schedule, but incorporating all the known Martin County record types encountered during recent records inventories performed with a sample of departments. The schedule has three main categories, General Record Series, Specific Record Series and Development Review Record Series.

Original records shall be retained according to the retention listed in the Record Copy designation for each Record Series contained in the schedule.

Most Duplicate records may be discarded after their administrative value has been exceeded. In other words, they may be disposed of after you no longer need them. For example – duplicates found in departments can include records such as payroll sheet dupes, invoice dupes, agenda item dupes, and so on.

NOTE: It is not necessary to submit a records disposition form to destroy duplicate records, but please verify that a record copy does in fact exist prior to such destruction.

The originator of any document generated is responsible for retention of that document. Retention of an executed (signed) copy of the document can be accomplished by establishing a centralized chronological file or by placing an executed (signed) copy in the subject file.

Records on County web page
Public records located on the Martin County Web page are unsigned duplicate copies of the original public records. These duplicates are provided for reference and convenience purposes only. Please be aware that:

1 - Once a public record has been placed on the Martin County Web Page it shall remain there indefinitely. The only exception to this rule will be made for records which have a statutory exemption to public access and have been placed on the Web Page in error.

2 - Alteration of public records located on the Martin County web page, or any public record, is prohibited unless specifically authorized via statutory exemption enacted by the Florida Legislature.

PROCEDURE
All records located on the Martin County web page are freely available for viewing and/or copying by the public. For access to the original public record, please contact the county department or staff member directly responsible for the content of the record. It is important to note that some of the original records represented on the web page may already have been dispositioned according to the General Records Schedule GS1-L published by the Florida Department of State, Division of Library and Information Services, Bureau of Archives and Records Management.

Records conversion service
The County uses Lason, Inc. of Miami Lakes, FL to convert paper records to microfilm or electronic format. County Departments are responsible for the cost of such services and should budget accordingly. The GSA schedule containing Lason’s services and costs may be accessed at the following link:
Guidelines for fulfilling public records requests.

Public records requests are regulated by state law. The County Administrator may, from time to time, direct that public records requests be handled in a specific manner in order to ensure that the public records are kept safe, to ensure that requests are complied with timely and according to law, and to ensure that material required to be kept confidential is not disclosed. Such directives must not be used in any way to hinder, delay or circumvent a person’s right of access to the public records nor to impede prompt and complete compliance with the Public Records Law.

The fact that the originator of a document requests that document remain confidential, does not in fact make that document confidential. It is still subject to the public records law unless the law makes it confidential or exempt. If a public record contains information that is confidential or exempt by law, then only the confidential portions of the record may be deleted. The remainder must be provided. No special interest in the subject needs to be shown by the requestor even if it is believed that the requests are made for the purpose of harassment. No automatic waiting period may be imposed. The only delay permitted is that which is reasonably necessary to allow the custodian to retrieve the record and delete those portions which are exempt or confidential by law. In addition, no arbitrary time period may be imposed during which public records may or may not be inspected (e.g. only between 1:30 and 4:30 pm).

The County may not refuse to provide a public record on the grounds that the record is also maintained by another agency.

DEFINITIONS

Public Records Request - One in which a person asks to view an existing file, map, photograph, film, document or the like; to listen to a tape; or to obtain copies of specific documents. This definition encompasses all materials made or received by an agency in connection with official business which are used to perpetuate, communicate or formalize knowledge. Persons have a right of access to any public record which is not specifically exempted or made confidential by law. A custodian of records is, however, not required to give out information from the public records, nor to produce an employee to answer questions, nor to provide lists of documents, all of which would fall into the category of a "request for information".

Request for Information - One in which the requested information does not already exist as a public record. For example, a person may request staff to create a document which does not already exist (perhaps by compiling certain information from other documents), or to provide a history or to research an issue. These types of requests are not covered by the Public Records Law and are not required to be honored by that law. Such requests by citizens may be honored by County staff, purely as a public service when the work can be accomplished quickly, or when answering requests of a certain nature are part of the duties and responsibilities of the department. Since requests for information are not covered by the Public Records Law (and need not even be answered under that law), there is no prohibition against how those requests must be made or complied with, except as may be provided by the County's own laws. Therefore, it is entirely appropriate to ask that such requests be put in writing.

PROCEDURE

The Executive Aide for each department will maintain a monthly log for public records requests. Each month Administration will print each department's log. The logs will be maintained in individual department subfolders in the directory. The log for each department will be named the calendar year (i.e. 2002, 2003, etc.). All of the logs for previous months will be retained in Administration. It is the responsibility of each department's Executive Aide to maintain a log each month. In the event that a public records request requires less than 15 minutes to produce, that item does not need to be logged. Please note that anytime a complex public records request is submitted directly to a department, the department should submit a copy to Administration. A complex public records request is defined as one that would require records from multiple departments or one that would require excessive time to compile.

Public records requests are not required to be in writing nor is the requestor required to disclose his or her name, address, or phone number. However, if a written request is received, a letter acknowledging receipt of the request should be sent to the requestor advising when the records will be available for review or pick up. Copies may be mailed upon receipt of copying charge.

A payment of 15¢ per page or 20¢ per two-sided copy shall be received and a receipt issued prior to providing copies. If records are voluminous or require the extensive use of information technology or personnel to produce or to assure that confidential material is deleted, a reasonable service charge may be imposed in addition to copying costs.
Records which are immediately available should be produced immediately. Where records are not immediately available, or will require examination for confidential or exempt material, they should be examined and made available as soon as reasonably possible. The requestor should be advised as to the time when the records are expected to be available for examination and the estimated cost of any service charge or copying charge. If a request is not sufficiently specific to identify the record, it is the responsibility of the County to notify the requestor that more information is needed.

Note: Within county departments and across the county there may be specific procedures that are used for records management at the department level. Those seeking information on such procedures should contact the appropriate department. Also see Existing Martin County policies for related information:

a - Public Records requests
b - Document Retention
c – Public Records on Martin County’s Web Page

Please direct any questions regarding this records schedule to the County’s Records Manager, x5480.

General Record Series

ACCOUNTS PAYABLE RECORDS
This record series consists of documentation of disbursements and the individual items leading to the summary information of payable records, including supporting documentation. The records and supporting documentation may include, but are not limited to, invoices, receiving reports, refund requests, travel records, vouchers and vendor files.

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ACCOUNTS PAYABLE/ RECEIVABLE SUMMARY RECORDS
This record series consists of summary documentation of receipts and disbursements. The records may include, but are not limited to, the vendor name, invoice number, date of invoice, check number, date of check and the amount of the check.

RETENTION:
a) Record copy. 10 years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ACCOUNTS RECEIVABLE RECORDS
This record series consists of documentation of receipts and the individual items leading to the summary information of receivable records, including supporting documentation. The records may include, but are not limited to, bad check records, invoices, receiving reports, refund requests, travel records, trial balance reports, and vouchers.

RETENTION:
a) Record copy. 4 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ADMINISTRATIVE CONVENIENCE RECORDS (THESE ARE DUPLICATE FILES – originals stored elsewhere)
This record series consists of a subject file, generally filed alphabetically, which is located away from the official files, such as in the Director's and other supervisory offices. The file contains DUPLICATES of correspondence, reports, publications, memoranda, etc., and is used as a working file or reference file on subjects which are currently significant or which may become significant in the near future. The material filed in this series is NOT the official file or record copy, but is maintained for the convenience of the officials in carrying out their elected or appointed duties.

RETENTION:
a) Record copy. Retain until obsolete, superseded or administrative value is lost.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ADMINISTRATIVE SUPPORT RECORDS (Miscellaneous records – but may have continuing value)
This record series consists of records accumulated relative to internal administrative activities rather than the functions for which the office exists. Normally, these records document day-to-day management of office personnel, including training; the expenditure of funds, including departmental budget work papers; supplies, office services and equipment requests; job requisitions which identify description of need, reason of need, requirements and copy of job description used to fill job vacancies within the agency; and receipts and other recorded experiences that do not serve as official documentation for audit purposes or of the programs of the office. However, because these records vary so greatly in content and value
(containing some duplicates and record copies), a relatively large proportion of them are of continuing value.

RETENTION:

a) Record copy. 2 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ATTENDANCE RECORDS: LEAVE INDEX (PRINTOUTS RECEIVED FROM PAYROLL WITH PAYCHECKS)

This record series consists of a summary of hours worked, leave hours used and accrued for all employees during a pay period. It also consists of the leave balances of vacation, sick and compensatory leave for all employees of the agency.

RETENTION:

a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ADMINISTRATOR RECORDS: PUBLIC AGENCY / OFFICIAL (Commissioner, County Administrator, Deputy County Administrator, Assistant County Administrator or Department Head records)

This record series consists of office files documenting the substantive actions of elected or appointed officials. These records constitute the official record of an agency's performance of its functions and formulation of policy and program initiative. This series will include various types of records such as correspondence; memoranda; statements prepared for delivery at meetings, conventions or other public functions that are designed to advertise and promote departmental programs, activities and policies; interviews; and reports concerning agency program development and implementation. The filing of these materials together in a central unified file is encouraged. These records may have archival value.

RETENTION:

a) Record copy. 10 years.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ADVERTISEMENTS: LEGAL (Required ads and/or announcements from newspapers)

This record series consists of advertisements which have appeared in newspapers on matters pertaining to the agency and other legal ads which may or may not indirectly affect the agency; i.e., bid invitations for construction jobs, public hearings or notices, and public sales. These records may also be part of another record series. A legal advertisement is frequently filed with the item to which it applies.

RETENTION:

a) Record copy. 5 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ATTENDANCE RECORDS: LEAVE (Leave requests created via WORD and signed)

This record series consists of requests or applications for vacation, sick, family medical leave (FMLA) and other types of leave including leave of absences, time sheets or timecards along with any required documentation (medical statements or excuses from a physician, jury duty summons, or military orders, etc.) submitted by an employee to document authorized absences.

RETENTION:

a) Record copy. 3 fiscal years provided applicable audits have been released and resolved.
c) Duplicates. Retain until obsolete, superseded or administrative value is lost.

BID RECORDS: CAPITAL IMPROVEMENT SUCCESSFUL BIDS

This record series consists of information relative to the processing and letting of capital improvement successful bids including legal advertisements, "Requests for Proposal," technical specifications, correspondence, "Invitations to Bid," bid tabulations and bid responses. "Capital Improvements" shall mean enhancement to buildings, fixtures and all other improvements to land.

RETENTION:

a) Record copy. 15 years after awarded provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

BID RECORDS: CAPITAL IMPROVEMENT UNSUCCESSFUL BIDS

This record series consists of information relative to the processing and letting of capital improvement unsuccessful bids including legal advertisements, "Requests for Proposal," technical specifications, correspondence, "Invitations to Bid," bid tabulations and bid responses. "Capital Improvements" shall mean enhancement to buildings, fixtures and all other improvements to land.
RETENTION:
a) Record copy. 5 fiscal years after awarded provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

BID RECORDS: NON-CAPITAL IMPROVEMENT
This record series consists of information relative to the processing and letting of successful and unsuccessful non-capital improvement bids including legal advertisements, "Requests for Proposal," technical specifications, correspondence, "Invitations to Bid," bid tabulations and bid responses.

RETENTION:
a) Record copy. 5 fiscal years after awarded provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

BUDGET RECORDS: APPROVED ANNUAL BUDGET
This record series consists of the approved annual budget and its' amendments. See also "BUDGET RECORDS: SUPPORTING DOCUMENTS." These records may have archival value.

RETENTION:
a) Record copy. Permanent.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

BUDGET RECORDS: SUPPORTING DOCUMENTS
This record series consists of any supporting documentation, budget matters and requests.

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

cALENDARS
This record series consists of a calendar showing official daily appointments and meetings. It may also include appointment books/planners that may or may not contain a listing of “prioritized daily tasks” and a calendar showing official daily appointments and meetings.

RETENTION:
a) Record copy. 1 year.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CASH COLLECTION RECORDS: RECEIPT/REPORT
This record series consists of, but is not limited to, receipt listings, register tapes, receipt books, validating machine tape records, deposit, withdrawal and transfer slips used to balance for cash deposits. See also “CHECK RECORDS.”

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CONTRACTS/LEASES/AGREEMENTS: NON-CAPITAL IMPROVEMENT
This record series consists of legal documents, correspondence, reports, etc., relating to the negotiation, fulfillment and termination of non-capital improvement contracts, leases or agreements to which the agency is a party. In addition, it includes the various contracts, leases or agreements entered into for the purchase of goods and services such as the purchase of gas, fuel oil and annual purchases of inventory-maintained items.

RETENTION:
a) Record copy. 5 fiscal years after completion or termination of contract/lease/agreement provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CORRESPONDENCE & MEMOS: ADMINISTRATIVE
This record series consists of routine correspondence and memoranda of a general nature that is associated with administrative practices but that does not create policy or procedure, document the business of a particular program, or act as a receipt. These records may have archival value.

RETENTION:
a) Record copy. 3 fiscal years.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

DIRECTIVES/POLICIES/PROCEDURES
This record series consists of the official management statements of policy for the organization, supporting documents, and the operating procedures that outline the methods for accomplishing the
functions and activities assigned to the agency. It includes all correspondence and memoranda generated relating to the policies and procedures, which are to be followed by employees. These records may have archival value.

RETENTION:

a) Record copy. 2 years after superseded or becoming obsolete.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

DISASTER PREPAREDNESS RECORDS: DRILLS
This record series consists of the results of disaster preparedness exercises and the supporting documents including scenarios, location of safety related drills, timetables, response times, probable outcomes, areas of difficulties, descriptions of how difficulties were resolved, and areas for improvement. The types of drills include: fire, tornado, safety, hurricane and chemical spills.

RETENTION:

a) Record copy. 2 calendar years provided reviews have been conducted.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

DISASTER RELIEF RECORDS
This record series consists of all supporting documentation that is related to the payment of state or federal funds received for natural or man-made disasters. The types of disasters include, but are not limited to, major storms, floods, fires, tornadoes and hurricanes. The records may also include applicable disaster relief funding agreements and expenditure reports. Supporting documentation may include, but is not limited to, copies of time sheets, payroll records, billing statements, receipts, purchases, executed contracts, invoices, canceled checks and daily activity reports.

RETENTION:

a) Record copy. 5 fiscal years after submission of final expenditure report or last payment is received, whichever is later, provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

DRAFTS AND WORKING PAPERS
This record series consists of documents, correspondence, memoranda, reports, and other materials in preliminary or developmental form before their completion as a final product. The drafts may include copies of materials circulated for review for grammar, spelling, and content. The working papers may include notes and miscellaneous documents and materials used in compiling and assembling the final product. NOTE: some draft documents and working papers may have long-term value; such documents may even have archival or historical value. Drafts of agency mission statements or preliminary versions of policy initiatives that could have a significant effect on a state or local government agency’s ability and responsibility to fulfill its function would qualify as records with a longer retention requirement. Such records might be better placed under the record series “ADMINISTRATOR RECORDS: PUBLIC AGENCY/ OFFICIAL.”

RETENTION:

a) Record copy. Retain until obsolete, superseded or administrative value is lost.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ELECTRONIC RECORDS SOFTWARE
This record series consists of proprietary and non-proprietary software as well as related documentation that provides information about the content, structure and technical specifications of computer systems necessary for retrieving information retained in machine-readable format. These records may be necessary to an audit process.

RETENTION:

a) Record copy. Retain as long as there are software-dependent records in storage.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.
a) Record copy. 3 years after completion of study provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

GRANT FILES: GRANTOR AGENCY/RECIPIENT
This record series consists of financial, management and any other related material that is generated subsequent to application for and/or expenditure of grant funds. These files include all funded applications, supporting documentation, contracts, agreements, and routine reports submitted by the grant recipient. Project completion has not occurred until all reporting requirements are satisfied and final payments have been received. Check with applicable granting agency for any additional requirements. These records may have archival value.

RETENTION:
a) Record copy. 5 fiscal years after completion of project provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

GRANT FILES: RECIPIENT
This record series consists of financial, management and any other related material that is generated subsequent to application for and/or expenditure of grant funds. Check with applicable granting agency for any additional requirements. Project completion has not occurred until all reporting requirements are satisfied and final payments have been received.

RETENTION:
a) Record copy. 5 fiscal years after completion of project provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

INCIDENT/INVESTIGATION REPORTS
This record series consists of reports of incidents that occur at a public facility or on publicly owned property, and the followup documentation created when an incident report is investigated. The reports may include, but are not limited to: the name of the reporting staff member; the date/time/location of the incident; persons involved or witnesses; the extent of the problem; emergency response, personnel notified, the general outcome of the incident; and any investigation that may follow.

RETENTION:
a) Record copy. 4 years.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

INFORMATION REQUEST RECORDS
This record series consists of correspondence accumulated in answering inquiries from the public. The series may include requests for publications or services provided by the agency, inspection and/or copies of public records, confirmation of meeting times/dates/locations, and requests for general agency information (i.e. mission statement, telephone list, map/directions, employee directory, etc.).

RETENTION:
a) Record copy. 1 fiscal year provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MAIL: REGISTERED AND CERTIFIED RECEIPTS
This record series consists of receipts for registered and certified mail sent out or received by a particular office. This record is often filed as part of another record series. See also “MAIL: UNDELIVERABLE FIRST CLASS,” “MAILING lists,” and/or “POSTAGE RECORDS.”

RETENTION:
a) Record copy. 1 fiscal year.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MAIL: UNDELIVERABLE FIRST CLASS
This record series consists of mail from any agency mailing that is returned. It does NOT include certified mailings that require proof of mailing.

RETENTION:
a) Record copy. 1 year after returned undeliverable.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MAPS: ORIGINALS
This record series consists of maps containing the original information and supporting documents in planning and engineering of local infrastructures and maps as required for the government land office, highway, sales, sectional, and geological surveys which are not required by statute or ordinance to be
filed with the Clerk of the Court. This record series does not include original maps that are filed with the Clerk of the Court.

RETENTION:
- a) Record copy. Permanent.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MAPS: SUPPORTING DOCUMENTS
This record series consists of copies of county/city right-of-way maps and other maps containing the original information and supporting documents in planning and engineering of local infrastructures and maps as required for the government land office, highway, sales, sectional, and geological surveys. This record series does not include the record copy of the maps/plats/right-of-ways that are filed with the Clerk of the Court.

RETENTION:
- a) Record copy. 15 calendar years.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MINUTES: OFFICIAL MEETINGS
This record series consists of any information which is the official record of meetings as defined in Florida Statutes Section 286.011(1) and (2); which may include transcriptions and/or agenda. These records may have archival value.

RETENTION:
- a) Record copy. Permanent.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MINUTES: OFFICIAL MEETINGS (HANDBRITTEN/ AUDIO/ VISUAL RECORDINGS)
This record series consists of handwritten, audio and/or visual recordings of official meetings as defined in s. 286.011(2), F.S.

RETENTION:
- a) Record copy. 2 years after adoption of the official minutes.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MINUTES: OFFICIAL MEETINGS (SUPPORTING DOCUMENTS)
This record series consists of supporting documents for minutes and agendas generated by official meetings.

RETENTION:
- a) Record copy. 3 fiscal years provided applicable audits have been released.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

MINUTES: OTHER MEETINGS
This record series consists of minutes and all supporting documentation from meetings which are not included in "MINUTES: OFFICIAL MEETINGS." These records may have archival value.

RETENTION:
- a) Record copy. 1 year.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PERSONNEL RECORDS: FLORIDA RETIREMENT SYSTEM
This record series consists of an application for employment, resume, personnel action reports, directly related correspondence, oath of loyalty, fingerprints, medical examination reports, performance evaluation reports, worker’s compensation reports, and other related materials within the Florida Retirement System (FRS). Note: Contact the Human Resources Office prior to destruction in case they wish to review the records.

RETENTION:
- a) Record copy. (Maintained by Human Resources) 25 years after separation or termination of employment.
- b) Duplicates. 1 year after termination of employment.

PERSONNEL RECORDS: NON-FLORIDA RETIREMENT SYSTEM
This record series consists of an application for employment, resume, personnel action reports, directly related correspondence, oath of loyalty, fingerprints, medical examination reports, performance evaluation reports, worker’s compensation reports, and other related materials that do not come under the Florida Retirement System (FRS). (Note: Contact your agency’s Personnel Office prior to destruction in case they want to review the records).

a) Record copy. 50 years after termination of employment.
b) Duplicates. 1 year after termination of employment.

PERSONNEL RECORDS: VOLUNTEERS/ TEMPORARY EMPLOYMENT
This record series consists of all information relating to each volunteer or temporary employee within an agency. Also, records may include an employment application and/or resume, personnel action forms and any correspondence relating to that individual. Volunteer employment may include, but are not limited to, name, address, and schedule of volunteer; training records; and emergency contact information. Temporary employment may include personnel from a local employment agency.

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PERSONNEL RECORDS: SCHEDULES
This record series consists of any scheduling documentation for shift or part time employees. These records may include hours scheduled to work, the switching of hours with another employee, the location or route of work assignment, and anticipated starting and ending times.

RETENTION:
a) Record copy. 1 fiscal year provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PURCHASING RECORDS
This record series consists of copies of purchase orders which are retained by the Purchasing Department or originating office while another is sent to the appropriate vendor for action. Included in this series is a log of outstanding and paid requisitions and purchase orders which are used for cross-referencing purposes. The series may also include requisitions which are sent by the originating office to supply, purchasing, graphics, duplicating or other sections for action. See also “ACCOUNTS PAYABLE RECORDS,” and/or “ACCOUNTS PAYABLE/ RECEIVABLE SUMMARY RECORDS.”

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PROJECT FILES: FEDERAL
This record series consists of original approved federal project contracts, agreements, awards, and line-item budgets, budget amendments, cash requests, correspondence and audit reports. (NOTE: Check with applicable agency and/or the Code of Federal Regulations (CFR) for any additional requirements.)

RETENTION:
a) Record copy. 5 fiscal years after completion of project provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PROJECT FILES: OPERATIONAL
This record series consists of, but is not limited to: work orders which identify department/agency requesting work/service; logs; project schedules, correspondence relating to the project, names of employees involved in project, equipment used, project tracking logs/reports, and other related information regarding the project such as fiscal year or year-end project costs.

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PROJECT FILES: NON-CAPITAL IMPROVEMENT
This record series consists of correspondence or memoranda (incoming and outgoing), resolutions, narratives, budget revisions, survey information, change orders, computer runs and reports, all pertaining to non-capital improvement projects and contract specifications for various proposed projects which may or may not be sent out for bid. The files may contain materials relating to specific projects provided by the agency.

RETENTION:
a) Record copy. 5 fiscal years after completion of project provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PUBLIC RECORDS REQUESTS
These are written requests from the public for access to or copies of specific records held by the department.

RETENTION:
a) Record copy. 1 fiscal year
b) Retain until obsolete, superseded or administrative value is lost

PURCHASING RECORDS
This record series consists of a copy of the purchase order that is retained by the originating office while the purchasing office sends another to the appropriate vendor for action.

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. 1 fiscal year.

SURVEYS/STUDIES: INTERNAL
This record series consists of raw data and work papers for any survey conducted to study management issues such as client/patron/employee satisfaction and service improvement. The data may include survey response cards, the results of telephone polls, tally sheets, opinion cards for suggestion boxes, and other records related to the study of operations. This does not include a consultant report. The final computation of the data is produced as a survey report and may be scheduled either as part of “Feasibility Study Records,” or “Operational and Statistical Report Records: Office,” depending on the nature and depth of the survey/study.

RETENTION:
a) Record copy. 1 calendar year after final data or report released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

TRANSITORY MESSAGES
This record series consists of those records created primarily for the communication of information, as opposed to communications designed for the perpetuation of knowledge. Transitory messages do not set policy, establish guidelines or procedures certify a transaction, or become a receipt. The informal tone of transitory messages might be compared to the communication that might take place during a telephone conversation or a conversation in an office hallway. Transitory messages would include, but are not limited to: E-mail messages with short-lived, or no administrative value, voice mail, self-sticking notes, and telephone messages.

RETENTION:
a) Record copy. Retain until obsolete, superseded or administrative value is lost.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

WORK ORDERS
This record series consists of information reflecting the individual history of major or minor maintenance or services requiring a work order request. Work order includes dates, locations, cost of labor, hours worked, equipment cost per hour, material used and cost, and pertinent details. This item does not include equipment maintenance records.

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Department Specific Record Series (Containing records not included in the General Record Series)

CONTRACTS/LEASES/AGREEMENTS: CAPITAL IMPROVEMENT
This record series consists of legal documents, correspondence, reports, etc., relating to the negotiation, fulfillment and termination of capital improvement contracts, leases or agreements to which the agency is a party. “Capital improvement” shall mean enhancement to buildings, fixtures and all other improvements to land. In addition, it includes contracts, leases or agreements with architects, engineers, builders, and construction companies.

RETENTION:
a) Record copy. 15 years after completion or termination of contract/lease/agreement provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

EXPENDITURE PLANS: CAPITAL IMPROVEMENT
This record series consists of capital improvement expenditure plans detailing the long-term building and capital improvement needs of the public agency. These plans may demonstrate a priority listing for capital expenditures as well as a time line for each project’s completion. These records may have archival value.

RETENTION:
a) Record copy. Permanent
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ORDINANCES
This record series consists of an official legislative action of a governing body, which action is a regulation of a general and permanent nature and enforceable as a local law. These records may have archival value.

RETENTION:
  a) Record copy. Permanent.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ORDINANCES: SUPPORTING DOCUMENTS
This record series consists of supporting documentation to the ordinance, which is a regulation of a general and permanent nature and enforceable as a local law. These records may have archival value.

RETENTION:
  a) Record copy. 5 years after adoption of ordinance.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PROJECT FILES: CAPITAL IMPROVEMENT
This record series consists of correspondence or memoranda (incoming and outgoing), drawings (or preliminary drawings), resolutions, narratives, budget revisions, survey information, change orders, computer runs and reports, all pertaining to capital improvement projects, construction and contract specifications for various proposed projects sent out for bid. The files may contain materials relating to specific projects, such as convention center, municipal/library, provided by the agency.

RETENTION:
  a) Record copy. 15 fiscal years after completion of project.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Administration – Office of Water Quality
See: Project files, Grant files, Administrative convenience records, Purchase order and Accounts Payable/Receivable records.

Administrative Services Department

INCIDENT/ INVESTIGATION REPORTS
This record series consists of reports of incidents which occur at a public facility or on publicly owned property, and the follow-up documentation created when an incident report is investigated. The reports may include, but are not limited to: the name of the reporting staff member; the date/time/location of the incident; persons involved or witnesses; the extent of the problem; emergency response, personnel notified, the general outcome of the incident; and any investigation that may follow.

RETENTION:
  a) Record copy. 4 years.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

INSURANCE RECORDS
This record series consists of insurance policies, claim filing information, premium payment records, cards and registers, etc. on agency’s property and/or employees. The series may also include all expenditures for insurance premiums shown as journal entries, the list of carriers and the amounts due to them.

RETENTION:
  a) Record copy. 5 fiscal years after final disposition of claim or expiration of policy provided applicable audits have been released.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

REAL ESTATE: COUNTY OWNED PROPERTY
This record series consists of, but is not limited to all documents concerning property owned by the County.

RETENTION:
  a) Record copy. For as long as Property is owned by the County.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

REAL ESTATE: APPRAISED PROPERTY NOT PURCHASED
This record series consists of, but is not limited to all documents concerning property that was appraised but not purchased by the County.

RETENTION:
a) Record copy. 3 fiscal years provided applicable audits have been released.
c) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Building

BUILDING PLANS: COMMERCIAL
This record series consists of graphic and engineering records that depict conceptual as well as precise measured information essential for the planning and construction of commercial buildings (blueprints, elevations, specification plans, etc.). The record copy is held by the local government permitting authority (Building Department). Other local governmental departments may hold duplicates for their reference use. Refer to Chapter 553, F.S.
RETENTION:
   a) Record copy. Retain for life of structure.
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

BUILDING PLANS: RESIDENTIAL
This record series consists of blueprints, elevations, specification plans and engineering records that depict conceptual as well as precise information for the construction of, or additions to residential buildings and single family residence. The record copy is held by the local government permitting authority (Building Department). Other local governmental departments may hold duplicates for their reference use. Refer to Chapter 553, F.S.
RETENTION:
   a) Record copy. 15 years after issuance of certificate of occupancy.
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PERMITS: BUILDING
This record series consists of permits issued by a governing authority for performance of construction, electric, plumbing, gas or mechanical work. Included in this series are the supporting documents and other permits that may be issued for construction or improvements to existing structures.
RETENTION:
   a) Record copy. 15 years provided applicable audits have been released.
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PERMITS: SIGNS
This record series consists of permits issued for installing/erecting signs. Included in this series are the applications and supporting documents. Refer to Chapters 125, 166 and 479, F.S.
RETENTION:
   a) Record copy. 3 years provided applicable audits have been released.
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PERMITS/ BUILDING: APPLICATIONS
This record series consists of an application that is completed when a licensed building contractor or mechanical contractor applies to construct structures of any nature. The application shows the date, the location, type of structure and plans, if required. The application may also include permits for gas, plumbing, electric and construction projects.
RETENTION:
   a) Record copy. 5 years provided applicable audits have been released.
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Community Services

CLIENT CASE FILES: HUMAN/ SOCIAL SERVICES
This record series consists of the client case files for citizens receiving assistance from a county or city social services agency. The series may pertain to, but is not limited to, low cost energy assistance programs, emergency payments for electric/medicine/medical care/food/rent, and referrals to a doctor or social services organization. The series may also include claim documentation and copies of monthly, quarterly and/or annual reports which are submitted by the local government agency to the State Agency for Health Care Administration.
RETENTION:
   a) Record copy. 4 fiscal years provided applicable audits have been released.
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CLIENT CASE FILES: VETERAN SERVICES
This record series consists of, but is not limited to, duplicates of the following documents: proof of military service; applications for various veteran administration (VA) benefits; marriage, death, divorce and birth
certificates; incoming and outgoing correspondence relating to the development and status of claims; change of address forms and all other VA forms which are used in development of claims for VA benefits. (No originals are contained in the files as all originals are forwarded to the Veterans Administration for processing). The series may also include a client case file index that may be maintained in hard copy and/or electronic format. The index may identify, but is not limited to the following: name, social security number, employment data, other sources of income, death records, and additional notes on pending claims.

RETENTION:

a) Record copy. 5 years after case closed provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

County Attorney’s Office

ANIMAL CONTROL RECORDS

This record series consists of copies of registrations, licenses, violation notices, tag receipts, rabies vaccinations certificates, neglect or abuse cases which have not resulted in litigation. These records are subject to audit by the Drug Enforcement Administration. Some records may be exempt from public inspection. Please refer to s. 381.0031(4), s. 828.30(4), F.S. and Rule 61G18-15.0071, F.A.C.

RETENTION:

a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

APPRAISALS: LAND (NOT PURCHASED)

This record series consists of documents pertaining to land not purchased by the county and all supporting documents.

RETENTION:

a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

APPRAISALS: LAND (PURCHASED)

This record series consists of documents pertaining to land purchased by the county. The series may include agency property deeds, appraisals, surveys, and other supporting documents.

RETENTION:

a) Record copy. Retain as long as agency retains property.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

BOND RESOLUTIONS

This record series consists of reports of principal, interest, paying agents and reports. The series documents legal agreements made to finance buildings.

RETENTION:

a) Record copy. Permanent.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

EASEMENT CONVEYANCES: SUPPORTING DOCUMENTS

This record series consists of duplicate easement conveyances and supporting documents. The official copy is recorded in the Official Records of the Clerk of the Circuit Court’s Office and then filed in a safe place with all other deeds and conveyances within the local government agency.

RETENTION:

a) Record copy. Retain until obsolete, superseded or administrative value is lost.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CODE ENFORCEMENT BOARD CASE FILES

This record series consists of case files of the Code Enforcement Board including affidavits, exhibits, letters, photographs, and orders. It may also include documentation and working papers which are used to complete the file.

RETENTION:

a) Record copy. 5 years after final disposition.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CODE VIOLATION RECORDS

This record series consists of documentation, such as photographs, on-site inspection notes, copies of the first and second violation notices, and may include orders to appear.

RETENTION:

a) Record copy. 3 years after final disposition.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CONTRACTS/LEASES/AGreements: CAPITAL IMPROVEMENT
This record series consists of legal documents, correspondence, reports, etc., relating to the negotiation, fulfillment and termination of capital improvement contracts, leases or agreements to which the agency is a party. “Capital improvement” shall mean enhancement to buildings, fixtures and all other improvements to land. In addition, it includes contracts, leases or agreements with architects, engineers, builders, and construction companies.
RETENTION:
  a) Record copy. 15 years after completion or termination of contract/lease/agreement provided applicable audits have been released.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CONTRACTS/LEASES/AGreements: NON-CAPITAL IMPROVEMENT
This record series consists of legal documents, correspondence, reports, etc., relating to the negotiation, fulfillment and termination of non-capital improvement contracts, leases or agreements to which the agency is a party. In addition, it includes the various contracts, leases or agreements entered into for the purchase of goods and services such as the purchase of gas, fuel oil and annual purchases of inventory-maintained items.
RETENTION:
  a) Record copy. 5 fiscal years after completion or termination of contract/lease/agreement provided applicable audits have been released.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ORDINANCES
This record series consists of an official legislative action of a governing body, which action is a regulation of a general and permanent nature and enforceable as a local law. These records may have archival value.
RETENTION:
  a) Record copy. Permanent.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ORDINANCES: SUPPORTING DOCUMENTS
This record series consists of supporting documentation to the ordinance, which is a regulation of a general and permanent nature and enforceable as a local law. These records may have archival value.
RETENTION:
  a) Record copy. 5 years after adoption of ordinance.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

LITIGATION CASE FILES
This record series consists of legal documents, notes, reports, background material, etc. created in the preparation of handling legal disputes.
RETENTION:
  a) Record copy. 5 years after case closed or appeal process expired provided applicable audits have been released.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

OPINIONS: LEGAL (ATTORNEY)
This record series consists of written opinions of lasting significance establishing policy or precedent answering legal questions from all program areas involving questions of interpretation of Florida or federal law. These records may have archival value.
RETENTION:
  a) Record copy. Permanent.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

OPINIONS: LEGAL (SUPPORTING DOCUMENTS)
This record series consists of the supporting documentation to the opinions that answer legal questions from all program areas involving questions of interpretation of Florida or federal law. These records may have archival value.
RETENTION:
  a) Record copy. 3 fiscal years provided applicable audits have been released.
  b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Development Files
(See Growth Management)

BRIDGE FILES
This records series consists of all documents associated with all bridges located within the county. They are maintained by the CIP programs assistant.

RETENTION:
   a) Record copy – Permanent
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CAPITAL PROJECTS - MAJOR ROAD PROJECTS
This records series consists of all documents associated with major road projects within the county. They are maintained by the CIP programs assistant.

RETENTION:
   a) Record copy - Permanent
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

COASTAL PROJECTS
This record series consists of, but is not limited to, documents relating to coastal projects.

RETENTION:
   a) Record copy. Determined by grant requirements
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

DEVELOPMENT REVIEW PROJECT FILES
This record series consists of application, site plan, plat, county permit, other permits such as SFWMD or DEP, correspondence, transmittals, environmental reports, PAMP (Preserve area management plan), meeting minutes from LPA and DRC. Added by Engineering: Signed Engineering approval, Inspection reports, and pre-construction meeting documentation including list of attendees.

RETENTION:
   a) Record copy - Permanent
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

EXCAVATION & FILL PERMITS
This records series consists of permits issued for the purpose of bringing fill or dredge fill of more than 100 cubic yards. They are maintained by the Devrev Permit Tech

RETENTION:
   a) Record copy – Permanent (Under review)
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

METROPOLITAN PLANNING ORGANIZATION (MPO) RECORDS
This record series consists of documents associated with the MPO including meeting agendas, meeting minutes, and studies such as the 20-30 plan and other future studies.

RETENTION:
   a) Record copy – Permanent (Under review)
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

PERMITS: EXCAVATION & FILL
RETENTION:
   a) Record copy. 3 years after project completion provided applicable audits have been released.
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

RAILROAD FILES
This records series consists of all documents associated with all railroads located within the county. They are maintained by the CIP programs assistant.

RETENTION:
   a) Record copy – Permanent
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ROAD FILES
This records series consists of all documents associated with specific roads within the County maintenance system. They are maintained by the Traffic administrative assistance.

RETENTION:
   a) Record copy – Permanent
   b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

U2/U1 PERMITS: RIGHT-OF-WAY
This record series consists of utility, state road and county road right-of-way permits from others allowing agency to cross the right-of-way.

RETENTION:
- a) Record copy. Permanent.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Emergency Services

RUN REPORTS: EMERGENCY
This record series consists of a report on patients who have been revived, or attempted to be revived, by the administration of drugs, both intercardiac and intravenously, and by using counter-shock treatment as well as all other patients who accepted service from an EMT, EMS or Air-Medical Provider, or a paramedic. Run reports will include patient's name, home address, age or date of birth, sex and race; call identification number, unit number of responding vehicles; transporting vehicle, if applicable; location of scene or incident; location of patient and destination of each call. The record copy of the run report is held by the service provider and a duplicate is sent to the Dept. of Health, formerly known as the HRS EMS Office.

RETENTION:
- a) Record copy. 5 years after last entry.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

RUN REPORTS: NON-EMERGENCY
This record series consists of reports on non-emergency miscellaneous runs where no treatment is rendered. This series is not used for the Department of Health's Run Reports or any report where medical attention, no matter how minor, was provided by the fire unit.

RETENTION:
- a) Record copy. 2 years provided applicable audits have been released.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

General Services

VEHICLE MAINTENANCE/ USAGE RECORDS
This record series consists of, but is not limited to, all records/logs/activity pertaining to vehicle maintenance and usage for gas, tires, repairs, fuel reports, vehicle usage activity, etc. used for agency cars.

RETENTION:
- a) Record copy. 3 fiscal years provided applicable audits have been released.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

VEHICLE RECORDS
This record series consists of all records pertaining to each vehicle owned by the agency. The series includes the vehicle registration papers, title, contracts, warranties, inspection information, maintenance agreements, credit card information, confidential tag issuance information and any other documentation relating to the vehicle.

RETENTION:
- a) Record copy. 1 year after disposition of vehicle provided applicable audits have been released.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Growth Management

CODE ENFORCEMENT BOARD CASE FILES
This record series consists of case files of the Code Enforcement Board including affidavits, exhibits, letters, photographs, and orders. It may also include documentation and working papers that are used to complete the file.

RETENTION:
- a) Record copy. 5 years after final disposition.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CODE VIOLATION RECORDS
This record series consists of documentation, such as photographs, on-site inspection notes, copies of the first and second violation notices, and may include orders to appear.

RETENTION:
- a) Record copy. 3 years after final disposition.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

COMPREHENSIVE MASTER PLANS: ADOPTED
This record series consists of adopted original and succeeding plans of local governmental agencies required by the State of Florida. The plans may contain elements such as growth management, sanitary sewer records, drainage records, future land use records, traffic circulation, economic assumptions, conservation, housing, recreation and open space, solid waste, electric utilities, potable water, intergovernmental coordination, mass transit and all other local governmental related functions. These records may have archival value.

RETENTION:

a) Record copy. Permanent.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

COMPREHENSIVE MASTER PLANS: ADOPTED (SUPPORTING DOCUMENTS)

This record series consists of supporting documents for original and succeeding plans of local governmental agencies required by the State of Florida. The supporting documents may include additional maps, surveys, site plans, correspondence, public opinion polls, copies of relevant studies or analysis, and other materials which support the proposed plan. These records may have archival value.

RETENTION:

a) Record copy. 5 years after adopted.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

DEVELOPMENT REVIEW PROJECT FILES (ALSO MAINTAINED BY ENGINEERING with additions)

This record series consists of application, site plan, plat, county permit, other permits such as SFWMD or DEP, correspondence, transmittals, environmental reports, PAMP (Preserve area management plan), meeting minutes from LPA and DRC.

RETENTION:

a) Record copy. Permanent
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

LICENSES: OCCUPATIONAL

This record series consists of applications, indexes and supporting documentation of licenses issued to business, professional, or occupation within “local governing authority's” jurisdiction.

RETENTION:

a) Record copy. 1 calendar year after expiration provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ZONING VARIANCE RECORDS

This record series consists of the zoning variance request, a copy of the final disposition and all other supporting documents such as determining records for zoning variances.

RETENTION:

a) Record copy. Permanent.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Information Technology Services

General schedule only

Library System

ACQUISITION RECORDS

This record series consists of records relating to the acquisition of library materials including, but not limited to books, periodicals, software, compact discs, videotapes, audiotapes, and film. These records may include the accession date, publisher and cost, date entered into or removed from the collection, and method of final disposal.

RETENTION:

a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

ANNUAL REPORTS

This record series consists of annual library reports relating to library statistics on expenditures, circulation, attendance, print and non-print inventory, services and/or programs and other pertinent information.

RETENTION:

a) Record copy. 3 fiscal years provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

CATALOG RECORDS
This record series consists of electronic or physical records identifying and describing books and other materials in library collections.

**RETENTION:**
- a) Record copy. Retain for life of material.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

**CIRCULATION RECORDS**
This record series consists of physical or electronic records of the loan of materials to library users, including records of overdue or delinquent materials.

**RETENTION:**
- a) Record copy. Retain until transaction completed.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

**EQUIPMENT USE RECORDS**
This record series consists of records of the loan or use of library equipment by the public and may include the loan or use of public access computers, DVD or video tape players, cassette tape recorders and film projectors.

**RETENTION:**
- a) Record copy. Retain until obsolete, superseded or administrative value is lost.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

**FINES AND REPLACEMENT CHARGE RECORDS**
This record series consists of records relating to payments for fines and replaced library materials and may include records relating to the withdrawal of materials from the inventory or catalog.

**RETENTION:**
- a) Record copy. 3 fiscal years provided applicable audits have been released.
- b) Duplicates. Retain until obsolete or administrative value is lost.

**INTERLIBRARY LOAN REQUEST RECORDS**
This record series consists of physical or electronic forms used by a library to request the loan of books or materials from another library.

**RETENTION:**
- a) Record copy. Retain until transaction has been completed.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

**PROGRAM REGISTRATION RECORDS**
This record series consists of registration records for library sponsored events and may include sign-up sheets or completed registration forms with participants' personal information.

**RETENTION:**
- a) Record copy. 30 days.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

**REFERENCE REQUEST RECORDS**
This record series consists of physical or electronic records of reference requests submitted by library users.

**RETENTION:**
- a) Record copy. Retain until obsolete, superseded or administrative value is lost.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

**USER APPLICATION: AUTOMATED SYSTEM**
This record series consists of forms submitted by individuals to request borrowing privileges from a library. Applications may include the individual's name, address, telephone number, date of birth, and/or social security number. For automated circulation systems the application may only be used to provide information for data input to establish electronic User Registration records.

**RETENTION:**
- a) Record copy. Retain until verification of data input.
- b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

**USER APPLICATION: NON-AUTOMATED SYSTEM**
This record series consists of forms submitted by individuals to request borrowing privileges from a library. Applications may include the individual's name, address, telephone number, date of birth, and/or social security number. For libraries using non-automated or manual circulation systems the application may also be used as the User Registration record.

**RETENTION:**
a) Record copy. Retain for 30 days after expiration.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

USER REGISTRATION
This record series consists of physical or electronic records that establish that an individual has library-borrowing privileges and includes the individual’s name and may include their address, telephone number, date of birth, and/or social security number. For libraries using manual circulation systems the application may also be used as the User Registration record.

RETENTION:
a) Record copy. Retain for 30 days after expiration.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.

Martin County Airport
None

Parks & Recreation
None

Utilities & Solid Waste
PERMITS: RIGHT-OF-WAY
This record series consists of utility, state road and county road right-of-way permits from others allowing agency to cross the right-of-way.

RETENTION:
a) Record copy. Permanent.
b) Duplicates. Retain until obsolete, superseded or administrative value is lost.
Commodity Technology Purchasing Policy

PURPOSE
This policy is intended to enable Martin County Staff to budget and purchase computer technology commodity items from departmental operating budgets. Items meeting the criteria set forth in this policy will not have to be processed through the Technology Investment Plan (TIP) amendment process.

POLICY
Martin County Staff will budget for and purchase small technology Commodity Hardware and Software in their departmental operating budget. Items that were planned and budgeted for in the TIP budget can still be acquired through the TIP budget. This policy also outlines how Commodity Hardware and Software can be purchased and the procurement process to support these transactions.

DEFINITIONS

PROCEDURE
The ITS (Information Technology Services) Catalog lists all approved Commodity Hardware and Software that can be purchased using this policy. These items shall not be purchased with "open" purchase orders. Items not listed in the ITS Catalog need to undergo an ITS review and approval before purchasing. Items must be purchased using the TIP account numbers and TIP activity codes outlined in this policy.

Commodity Hardware
Purchase of Commodity Hardware that is included in the ITS Catalog does not require a TIP amendment, budget transfer or administrative approval. Commodity Hardware shall be purchased from departmental operating budgets and includes handheld computing devices, cameras and other small items in the computer technology hardware category. The unit price threshold is $750 with an aggregate annual purchase of up to $5,000, per department. These items must be purchased using correct TIP account number and the Departmental Computer Hardware and Software TIP (T01007) activity code.

Commodity Software
Purchase of Commodity Software that is included in the ITS Catalog does not require a TIP amendment, budget transfer or administrative approval. Commodity Software shall be purchased from departmental operating budgets and includes single copies of office productivity software required for individuals to perform their jobs. The unit price threshold is $500 with an aggregate annual purchase of up to $3,000, per department. These items must be purchased using correct TIP account number and the Departmental Computer Hardware and Software TIP (T01007) activity code.

Copiers and Fax Machines
Copiers and fax machines are not TIP items and should be budgeted and, purchased or leased, using the normal operating department budget accounts. These items must be purchased on their own purchase order.

Laptops
Laptop purchases will require a TIP amendment, budget transfer and administrative approval. Laptops shall be purchased using the appropriate TIP account number and the Departmental Computer Hardware and Software TIP (T01007) activity code. However, if a laptop that is being purchased is going to be used as a Desktop Computer, only a budget transfer is required for the amount above the standard desktop configuration cost. The existing desktop will be returned into the desktop fleet for re-assignment. The laptop shall be purchased using appropriate TIP account number and the Computer Desktop Fleet Replacement TIP (T04004) activity code.
“all_martin” E-Mail Policy
PURPOSE
The “all_martin” E-Mail list reaches everyone who has a County E-Mail address and is maintained by Information Technology Services.
POLICY
“all_martin” E-Mails are sent to advise all Martin County employees (which includes the Constitutional Officers and their staff) of items affecting or potentially affecting all Martin County employees. Such items may include but are not limited to: computer software updates (when different computer software will be unavailable), a special benefit that only County or government Employees may obtain (discounted fees to a health club/gym, theme park, cellular phone services, etc.), employee benefits updates/notifications, County sponsored events (ie Vendor Day, Safety Day, Benefits Day), or any notification when the County or a Constitutional Officer are the agent/sponsor (ie annual United Way campaign). Prior approval must be obtained to send an “all_martin” E-Mail from the Assistant to the County Administrator or his/her designee. E-Mails affecting only the Administrative Building, for example, should not be sent to "all_martin" as it does not apply to all remote locations of the County.
Cellular Telephones

PURPOSE
This policy is intended to establish uniform practices for use of cellular communications technologies, i.e. cellular telephones. In the course of carrying out job responsibilities, there may be a need for work related communications while away from the office or primary work location. As cell phones are becoming a preferred method for personal communications as well, it is becoming cumbersome to have separate cell phones for business use and for personal use. Therefore, the BOCC will not purchase cell phones, or enter into cell phone contracts, to be used by employees for business related purposes. The BOCC may agree to pay a cell phone stipend for a cell phone package purchased by an employee.

POLICY
A monthly stipend will be issued to County staff that is in positions authorized for BOCC cellular phone usage. Positions authorized for BOCC cellular phone usage are determined by the criteria established by the Leadership Team. The criterion is as follows:

• Safety requirements indicate having cellular phone is an integral part of performing duties of job description.
• More than 50% of work is conducted in the field.
• Required to be contacted on a regular basis. (No office)
• Required to be on-call (24/7)
• Critical decision maker

The following positions are eligible for the cellular phone monthly stipend:
1. County Commissioner, County Administrator, Assistant County Administrator, County Attorney, and Department Executives.
2. County Staff including: designated IT staff, designated maintenance staff, designated security staff, and other designated staff as authorized by the respective Assistant County Administrator.

The following guidelines must be followed for employees assigned to the stipend plans:

• BOCC will not be responsible for procuring cellular phone accounts and equipment for those individuals that are eligible for the monthly stipend.
• The cellular phones will not to be purchased by, licensed or directly billed to BOCC entities for those individuals that are eligible for the monthly stipend. BOCC will not pay for any cell phone equipment or related service plans. The individual in the authorized BOCC cellular phone usage position will be responsible for choosing and paying for cellular phone equipment and services.
• Cellular phone service will not be purchased by, or directly invoiced to BOCC entities for those individuals that are eligible for the monthly stipend. The monthly stipend is taxable income; therefore the individual will be taxed according to the regulations of the IRS code.

Reimbursement Rates:
The BOCC monthly stipend payment rates are as follows:
$30 Stipend: This stipend is for the employee who has light to moderate usage of the cellular phone for business purposes, or may have heavy usage, but primarily in the local calling area. The employee may agree to allow the BOCC to publish their cellular phone number for public access.
$40 Stipend: This stipend is for the employee who has moderate to heavy usage of the cellular phone for business purposes, or may have light usage, but frequently travels out of the local/regional area. The employee must agree to allow the BOCC to publish their cellular phone number for public access.

The County Administrator may authorize a different stipend (lower or higher) in special circumstances, on a case by case basis.

PROCEDURE
Cell Phone Reimbursement Procedures:
• BOCC employees who are eligible for a cell phone stipend will be required to submit the Cellular Phone Stipend Request Form to their Department Director or Designee. The Department Director or Designee will complete the Authorization Form and insert the monthly stipend amount (based on past usage). The appropriate Assistant County Administrator must authorize the request. After the request is approved the Department will process an EPAF for the employee’s stipend. Note: Exceptional usage situations may require cellular phone service beyond the normal usage and control of the individual.
When the BOCC has agreed to pay an employee for business related cell phone usage, such payment will be made to the employee in the form of payroll stipend.

Because cell phone service is a contractual agreement between the cell phone service provider and the employee, the BOCC does not recommend or prefer any particular vendor. The choice of service providers is strictly up to the individual employee. However, some vendors will offer discounts to individuals who inform the service provider of their affiliation with Martin County BOCC.

Any stipend agreement will be immediately cancelled, and payroll payments immediately terminated, whenever an employee receiving a cell phone stipend terminates employment with the BOCC. Any such stipend will also be cancelled if an employee changes job positions. In such case of a change in job positions, a new Cellular Phone Stipend Request Form must be approved to establish the continued business need for a cell phone.

Bills for exceptional usage or special services required may be submitted to the Accounting Department once approved by the employee's Department Director or Designee. An example would be when an individual who is already receiving a cellular stipend of $40, travels out of town to a conference. If during the conference, an issue critical to BOCC operations occurs, and the employee must use the cellular phone extensively to respond to the situation, the employee will most likely incur costs exceeding the $40 in business usage time for that month. They employee would submit copies of their bill for reimbursement of related changes.

All costs related to the purchase and usage of the cellular phone is the responsibility of the employee.

Tools of the Trade. Where specialized cellular phone equipment (SmartPhone, BlackBerry) and/or services (text messaging, GPS) are required by the County for specific duties, the County may opt to provide or reimburse employee for the special cellular equipment and/or phone service, upon written approval of the County Administrator.

Pool Phones. Department Directors may opt to have a minimal amount of departmental pool phones. Pool phones are restricted to the free phones, if available, if not the lowest priced phone. These will be used on a “check-in” and “check-out” basis, for the purpose of providing the department with the ability to communicate with their employees in the field, but are not assigned to an individual.

CELLULAR PHONE STIPEND AUTHORIZATION FORM
Employee Name: _____________________________________
Department: __________________________________
Budget account: _ _ _ _-_ _ _ _-_ _ _ _ _-_ _ _ _ _
Date cellular service to begin: _ _ / _ _ / _ _
Cellular phone number: ( _ _ _ ) _ _ _ - _ _ _ _

Stipend Amount:
___ $30 light to moderate usage of the cellular phone for business purposes, or may have heavy usage, but primarily in the local calling area.
___ $40 moderate to heavy usage of the cellular phone for business purposes, or may have light usage, but frequently travels out of the local/regional area.
___ $ tools of the trade, Pool Phones or other levels of re-imbursement, as the County Administrator approves.

Employee Certification
I certify that the above stipend will be used toward expenses that I incur for cellular phone usage for business purposes. I further certify that should the business usage significantly decline for a sustained period, that I would notify my supervisor, in writing, as soon as practicable. I understand that this stipend will be included on my W-2 form as taxable income. I further understand that the BOCC is not responsible for the tax consequences of the stipend or the business use of my personal cellular phone.
After Hours Backup

Computer problems encountered by the Department of Cultural Services would be handled by their staff member(s) using an IT call roster. Calling individuals on the roster does not guarantee support, but more than likely would be sufficient in meeting their requirements. In the event that the Prairie Center can not reach an IT technician on the call roster, they can call the Police department and have the on call technician notified.

Any technician that is called into the Police, Fire, or Prairie Center Departments will receive a minimum of two hours pay at one-and-a-half times their hourly rate. For calls resolved over the phone, the technician will be paid and the technician will log the time to the nearest ¼ hour. The Village of Schaumburg does not compensate staff members for travel to and from work, or for being on call unless they are actually called in or do work.

Any overtime worked as a result of these procedures will need to be recorded as a CSR, and filed through the normal payroll process by submitting hours to the Information Technology Administrative Secretary who will submit the hours to Human Resources for the next payroll.
013 Village of Schaumburg, IL – After-Hours Computer Support Policy

013 Village of Schaumburg, IL – After-Hours Computer Support Policy

After Hours Computer Support Policy
Purpose
To define the parameters by which user departments will be given computer support after normal work hours.
Currently, Information Technology provides computer support from 7:00 a.m. until 6:00 p.m., Monday through Friday. Computer usage by user departments has steadily grown over the years and is now to the point that some departments need computer support beyond the typical work day. In order to facilitate this needed computer support, Information Technology will be scheduling at least one technician to take off-hour calls for the village departments. Technicians who are scheduled for call will be required to carry pagers and be available for calls if needed. The department needing assistance will contact the scheduled technician and if the problem cannot be remedied over the phone, the technician will come in and correct the problem.
The application development team will provide full availability to its customer base via physical presence in the office, electronic mail, the Banner hotline (x3839), and the use of a pager.

User Procedures

Users should continue to request service or report problems in the same manner they are accustomed to. For routine questions, such as checking the print queue in Banner, the user should call the Banner hotline. For more specific problems with applications, the user may call, e-mail, or visit the applicable application development team member.

During working hours, given the user’s problem is not preventing them from working, the user should leave a voice mail on the Banner hotline, if applicable, or leave a voice mail or e-mail for the appropriate team member, if the team member is not present.

During working hours, given the user’s problem is preventing them from working and must be corrected immediately, the user should call or visit the application development team supervisor, if the appropriate team member is not present. If the supervisor and no team members are present, the user may escalate to the IT director or his/her secretary. The on call application development team member will be paged at this time.

During non-working hours, a problem is typically reported to the technical support staff. This process does not change. If the technical support person determines a problem call should be routed to application development, they will use the prescribed guidelines for handling the call.

The Banner hotline will be programmed such that when a voice mail is left, the on call application development team member will be paged.

Technical Support Procedures

The technical support staff will page the on call application development team member. The on call application development team member should use the prescribed guidelines for handling the call. If the application development team member does not respond within one-half hour of being paged, the application development supervisor should be called. The application development supervisor will handle or route the problem in the same manner the on call application development team member would. If the application development supervisor does not respond within one-half hour of being called, the problem should be escalated to the IT director.

Application Development Team Procedures

If the on call application development team member is paged because a voice mail message has been left on the Banner hotline, the team member should pick up the message from voice mail and handle the call accordingly.

If the on call application development team member is paged by a technical support person, by the team supervisor, or by the department director or secretary, the team member should return the call within one-half hour and handle the situation accordingly.

The on call application development team member should address the call in the following manner:

* Gather the end user’s name, department, phone number.
* Gather the name of the application and the exact error that occurred.
* Identify the urgency of the problem (is their work stopped, when do they need it corrected, and the impact of not correcting).
* Identify if they can handle the situation themselves or if they need to route the problem to another team member. The application development supervisor may be consulted if necessary.
* Establish with the end user who will be contacting them regarding resolution and an approximate time frame that they will be contacted.
* Handle the problem or contact the appropriate team member for resolution. If the appropriate team member cannot be reached for one-half hour, the call may be escalated to the application development supervisor, depending upon the urgency. If no team member or the supervisor cannot be reached for one hour, the call may be escalated to the IT director, depending upon the urgency.
As always, should any team member be required to go into the office during off hours to resolve a problem, normal overtime rules will apply.

General

It is the responsibility of the application development supervisor to plan the schedule for rotating the pager among team members. The schedule will be determined by availability, meaning vacations and other time off, will be considered.

It is the responsibility of the application development supervisor to publish the on call schedule at least once a month (and if the schedule changes at any time during the month) to the IT director, to the IT secretary, and to the technical support supervisor.
Requests for Customized Software Applications Policy

Purpose
To provide guidelines for requesting computer programming service utilizing internal and external programming resources. All contracts for custom software will include certain requirements aimed at insuring quality design and documentation as well as illustrating a clear distinction of the responsibilities being shared between the Village and the service provider.

Guidelines and Procedures
1. The Director of Information Technology is responsible for approving all departmental computer programming requests, unless the programming is done through an existing agreement with a vendor (e.g., SCT, ACS, Printrak); provided however, that any modifications to existing agreements shall be approved by the Director of Information Technology.
2. In-house programming is available for departments wishing to create applications specific to their recommendations. Because this service is limited by time constraints and available staffing, departments will be served on a priority basis decided on by the Director of Information Technology.
   a. All requests for in-house programming projects should be submitted to the Information Technology Department using a System Service Request (SSR). The SSR is an on-line Lotus Notes system where software development projects are entered and tracked through the life of the project.
   b. A description of the program’s goals and objectives should be submitted along with samples of desired menu screens and report formats. The request must give Information Technology staff enough information to make a decision as to how long the project will take, the required resources, and the complexity of the project. All training requirements must be spelled out as well.
   c. Upon review by Information Technology staff and approval of the project by the Director of Information Technology, a mutually agreeable time table will be established with the department requesting the creation of the custom application.
   d. Upon completion of the project, documentation and training for the software application will be provided if applicable. The department as well as Information Technology, are responsible for the successful implementation of the project and must work with the programmer to accomplish all goals.
3. Outside custom programming is encouraged by departments developing complicated or time consuming applications. Due to limited in-house programming resources many departments will find it beneficial to contract with an outside vendor to achieve special purpose programming applications within the individual departments.
   In such instances, the following requirements shall apply:
   a. All custom applications to be created by outside vendors and items b though h below must be reviewed and approved by the Director of Information Technology prior to creating a purchase order, signing any contract, or allowing work to begin.
   b. These custom applications must be written using approved software standards (e.g., Oracle, Lotus Notes, etc.), and must be compatible with current Village systems and future development plans as defined by the Director of Information Technology.
   c. All recommendations must include a statement of programming objectives, including as much detail as is available about the activity which is to be computerized. Specific screens, reports, and other requirements along with the examples of data to be captured must be included.
   d. All recommendations must include specifications for documentation to be provided by the vendor including the scope and subject areas the documentation is to cover with final documentation included as a deliverable.
   e. All recommendations must include a schedule indicating the initial delivery date, testing periods and expected date of completion, time tables and arrangements for ongoing support and training must also be established and explained.
   f. All recommendations should include a narrative explaining the amount and types of training expected for the program.
g. All recommendations must include a not-to-exceed cost figure for the project. This figure must be agreed to by the vendor and a signed proposal must be included.

h. Any customized programs written exclusively for the Village shall remain the property of the Village and the person creating or recommending the programs shall have no property interest therein.

i. The finished product must work (e.g., meet the objectives set in item -c- above). In order to ensure that the product works, final payment will not occur until all corrections to the product are made and when the test period, as stated in paragraph e, is completed.

j. Information Technology is in charge of all software applications projects. Information Technology will work with requesting departments in establishing the application requirements. Information Technology will budget for the project as part of the annual budget process.
Electronic Mail Usage Policy

Purpose
To provide guidelines for the secure, effective, and efficient use of the Electronic Mail System. It sets forth the Village’s policy with regard to access to and disclosure of electronic mail messages sent or received by Village employees using the electronic mail system. This system provides inter and intra departmental communications for authorized users.

Guidelines and Procedures
1. The electronic mail system is a user friendly, privileged communications system that electronically creates, stores, and forwards communications and data from one user to one or more users.
2. Authorized users will be provided a login name which allows access to one of the Village’s local area networks. The user will then provide a personalized Network Password. The confidentiality of this password will be the sole responsibility of each user. Any communications via the electronic mail system will be attributed to the login name of the originating user. Users may wish to utilize any additional security features built into the electronic mail system (i.e., passwords, encryption, etc.) to further protect their individual messages.
3. The Village reserves the right to monitor electronic mail messages.
4. The Village reserves the right, with Village Manager approval, to access and disclose the contents of any employee’s electronic mailbox. Such access may occur, but is not limited to, the Village’s need to investigate a possible violation of policy or a breach of the computer or electronic mail system security. Any contents properly obtained under these guidelines, may be disclosed within the Village without the consent of the employee, but only to those employees who have some reasonable need for access to the information, and after Village Manager direction. The contents may also be disclosed outside the Village, if needed, with the permission of the Village Manager.
5. To maintain the security of the system, each user shall be required to log out of the system if they are not in physical control of the computer and know they will be away from the computer. If a user fails to observe the recommended log out procedure, other users may have easy access to messages stored in their mailbox.
6. No user shall divulge his Network or Notes password unless to authorized support personnel. Any person with knowledge of any password not his/her own shall report this to his/her supervisor immediately. The supervisor will then take the appropriate actions for securing the system.
7. No employee shall attempt any unauthorized access to the electronic mail system. Any employee found to have engaged in unauthorized access of the system may be disciplined.
8. No employee shall use the electronic mail system for mass distribution of personal or non-business information. These messages include, but are not limited to, those messages containing personal advertisements, personal opinions or personal requests. The Village maintains a separate Trading Post database for these items.
9. Initial access for new users, will be authorized and recommended by the employee’s department head and through their respective user group representative. A legitimate business need must be demonstrated to obtain access.
10. Initial training shall be provided by Information Technology or trained departmental staff where possible.
11. The maintenance of the master address and public group lists used on the system shall be Information Technology’s responsibility. Suggestions for changes should be forwarded to the employees’ respective user group representative for their recommendation.
12. No electronic mail system shall be used to send copies of any documents in violation of copyright laws.
13. No employee with authorized access to the electronic mail system shall allow an unauthorized person, employed or not employed by the Village, to use the system for any reason.
Requests for Hardware and Peripherals Maintenance/Repair Service Policy

Purpose
To provide guidelines for requesting computer products, maintenance and/or repair service. Establishing guidelines will facilitate tracking of computer product repairs and reduce work disruption caused by computer-related problems.

Repair Service
A. Village employees should immediately notify the Information Technology Department when a computer equipment problem occurs by calling the x3838 Help Desk Line.
B. Information Technology personnel will log the problem and assign it to a technician within 15 minutes of receiving the call or message.
C. In the event that a hardware component has to be ordered, the user will be notified and supplied with loaner equipment.
D. Within 2 business days of the new equipment arriving, I.T. will replace the loaner equipment.
E. All repairs or new installs will be tested before a customer ticket is closed.
Hardware Standardization Policy

To ensure long range, cost effective computer hardware configurations for the Village of Schaumburg. General hardware standards will be established to ensure hardware compatibility across all Village departments. It is the goal of the Village to reduce training costs, supply costs and maintenance costs through the use of similar and compatible equipment.

All computer equipment to be purchased, including personal digital assistants (see attached addendum regarding PDA’s), will be reviewed by the Director of Information Technology to insure compatibility with other Village systems. A determination will be made based on the type of equipment, its use, its potential maintenance liability, any previous Village experience with the product, the vendor support available and its relationship to other equipment already owned by the Village. Obviously, cost will also be considered as a factor when accessing various types of equipment.

All requisitions regarding computer hardware and peripherals will be reviewed for approval by the Director of Information Technology. Complicated proposals should be forwarded to the Director of Information Technology early in the research process to avoid last minute problems with compatibility.

The intent of this policy is to ensure that all hardware is compatible with other Village systems. It is not intended to impede the initiative of departments wishing to computerize applications. Departments are encouraged to pursue additional computerization, but must coordinate with the Director of Information Technology to meet these goals.

Since the Information Technology Department realizes that Personal Digital Assistants (PDAs) provide many benefits to their owners at a reasonable cost, it is IT’s intention to support PDAs as much as possible. This includes PDAs that are owned by Village employees who wish to use them as part of their daily work routine.

There are, however, risks involved when using personal equipment on the Village’s system. In order to find a good balance between convenience and productivity for Village employees while minimizing the risk to Village systems and burden to IT support staff, the following are the guidelines that all employees who wish to use their PDA to synchronize with Village systems must agree to:

A. All employees who wish to connect their personal PDAs to Village equipment must obtain authorization from their appropriate department head as well as from the IT Director.

B. The IT Department will only allow Palm-based PDAs to connect to the Village’s system. This includes all Palm OS PDAs with operation system versions 3 or greater (e.g., Palm III, Palm V, Palm m100, etc.).

C. The IT Department will provide the synchronization software to synchronize to the Village’s systems. In agreement with the existing IT software policy, village employees are not to bring in software from home and install it on their PCs to support their PDA without first obtaining permission from the IT Director.

D. The Employee will provide the cradle or synchronization cables as required. The IT department will not provide this.

E. The IT department will not provide training on how to use the PDA.

F. The IT department will support the user in connecting the PDA to the village systems, but will not be able to provide support for the PDA itself nor for the applications used in conjunction with the PDA.

G. The IT department will not be responsible for the data maintained on the PDA. This includes both personal and village data. It is the village employee’s responsibility to take appropriate actions to back up the PDA data.

H. The IT department will not be responsible for damages that may occur to equipment or data whether personal or village-owned.

I. The IT Department reserves the right to remove connectivity of a personal PDA to the Village’s network if there is sufficient reason to believe there is a potential risk to Village equipment, systems, network or data (i.e. Virus or worm threats, damaged hardware, security risks, etc.).

J. The employee agrees to not synchronize data to/from the PDA that would violate the Village’s Acceptable Use policy (e.g., Pornography, explicit content, racially-insensitive content, etc.).

I understand and agree to these guidelines:
IT On-call Protocol
For On-Call support of the Village computer systems, please follow the procedures outlined below:

On-Call Technical Issue Procedure
1. Call the IT On-Call Pager at (847) 547 – 4936. At the tone, enter your phone number and press the pound (#) symbol. Or you can send a message to the pager via Lotus Notes. The address is: “Pager – On Call for IT Techs”. Indicate the issue in the message. Please allow for 15 Minutes for a reply. If no reply to the first attempt, please try paging again allowing for a second 15 minute time interval.
2. If no response to either pager attempt, please contact the Technical Supervisor, Vince Sifuentes at (847) 344-5270 (mobile phone), or by Direct Connect Alert – 3813. Please allow 30 minutes for a response.
3. If no response to the above, please contact the Assistant Director of IT, Chris Westgor at (847) 878-2171 (mobile phone), or Direct Connect – 2171. Please allow 30 minutes for a response.
4. In case none of these procedures produces a resolution to the issue, then contact the Director of IT, Samuel Ferguson at (847) 344-5267 (mobile phone), or Direct Connect – 3800. Please allow 30 minutes for a response.

After Hours Policy
If it is determined that an on-site repair is required, the On-Call technician will be expected to arrive within two (2) hours of the original page/notification.
Any technician that is called will receive a minimum of two hours pay. Time-and-a-half pay will begin once a cumulative hourly total for the week exceeds 40 hours. For calls resolved over the phone, the technician will log and be paid for the time to the nearest ¼ hour. The Village of Schaumburg does not compensate staff members for travel to and from work, or for being on call unless they are actually called in to do work.
Any overtime worked as a result of these procedures will need to be recorded as a CSR, and filed through the normal payroll process by submitting hours to the Information Technology Administrative Secretary who will submit the hours to Human Resources for the next payroll.
A pager will be issued to the technicians on a rotating weekly basis, assigned by the Technical Supervisor. Any technician found to be intentionally not answering the pager, will be subject to disciplinary action.
New Hire / Transfer / Move Requests

Purpose
To provide computer setup of equipment, peripheral, software, and network connection to new employees or employees who are transferring to another department or changing locations within their current department.

Guidelines and Procedures
Requests for new hires, transferring employees, or employees moving within their department will be submitted to the Information Technology Department three days in advance of the employee's start date.
A. HR will generate the New Hire / Move (Transfer) form and submit the form to the hiring supervisor.
B. The hiring supervisor will complete the form and submit it to I.T. no later than 3 days in advance of the employee's start date.
Example Problem Resolution Scenario:
Joe Employee's phone does not work
1. Call Nextel for assistance;
   - If helped, problem resolved – Complete
   - If problem persists and is told it is broken, call IT
2. IT assesses and directs employee to Prime Wireless for repair;
   - IT gives employee replacement phone
3. Phone fixed or temporary given to employee (loaner);
4. If phone needs replacing, department submits request to Manager’s Office for purchase via the cellular phone administrative protocol. Upon approval;
5. Employee’s department prepares requisition and forwards to Finance with the Manager’s approval attached as backup;
6. Finance orders phone;
7. IT sets up phone and routes to employee retrieving loaner phone;
Administration:
* IT will administer all phones
* Finance will administer all phone plans and cost and inventory lists
* IT and “helper” departments will make phone changes electronically with IT monitoring the Nextel activity report
Organizational Strategy Policy

Purpose
To establish a set of policies and procedures for microcomputer use within the Village of Schaumburg so that each department has guidelines to follow in their normal day-to-day computing activity. These guidelines establish the organizational roles played by the Director of Informational Technology, his staff, and each department.

Guidelines and Procedures
The Director of Information Technology is responsible directly to the Village Manager for the management and coordination of all Village Information Technology activities and is authorized, with the Management’s concurrence, to establish organizational policies and procedures related to Information Technology. The organizational strategy of how these policies and procedures come about and how they are to be administered is as follows:

1. All Policies and Procedures are to be administered and approved by the Director of Information Technology and the Village Manager.
2. The Director of Information Technology will have a computer users group which consists of computer user representatives from each department.
3. Policies and Procedures may be derived from many varied sources, including suggestions by employees to the computer user representative of the employee’s department. If the department representative feels the suggestion has merit, he/she shall forward the suggestion to the computer users group and Director of Information Technology.
4. Proposed Policies and Procedures forwarded to the users group shall be discussed and approved by the Director of Information Technology. Formal policies approved by the Village Manager shall be distributed to all departments through the department heads and updated in the policy database.
5. The Director of Information Technology is available to answer or clarify any questions concerning these Policies and Procedures.
Office Equipment/Technology Replacement

The Village of Schaumburg aspires to provide its employees with office equipment/technology equipment that enable them to offer effective and efficient services that our residents demand, while applying sound business approaches associated with: understanding the costs and benefits of office equipment/technology and its capabilities; funding purchases through the accumulation of resources as much as practical, and making decisions on replacements considering the level of usage, performance, and changing industry standards.

Expenditures: The General Office Equipment/Technology Replacement Fund shall be used to finance all office equipment/technology items which have met or exceeded their effective useful life as established by policy. Items that have exceeded established thresholds but which are still useful will be replaced upon the first major repair occurrence or when minor repairs outweigh the benefits of a new purchase. Replacement item’s subject to financing through this policy shall include, but are not necessarily limited to, the following categories of equipment:
- Computer Central Processing Units (CPU’s)
- Monitors
- Printers
- Copiers
- Audiovisual Equipment
- Telecommunications (phone/phone switches)
- 911 Emergency Dispatch Equipment (Communication Center Equipment)
- Other Office Equipment
- Other Communication Equipment

Funding: General Office Equipment/Technology Replacement Fund: The repository of the reserves for future office equipment/technology replacements is known as the General Office Equipment / Technology Replacement Fund. The purpose of the fund is to provide assured and adequate resources for the future replacement of office equipment and technology equipment, not subject to the financial constraints of the General Fund. Upon acquisition, any technology equipment with a purchase value in excess of $150, the village’s threshold for tracking insurable equipment, or greater and an expected life in excess of one year shall be automatically included in the General Office Equipment/Technology Replacement Fund for future replacement, and the appropriate replacement charge will be collected from the fund from which the benefiting department derives its funding. The intent of the low threshold is to include all low cost equipment items that may have high volume quantities (computer monitors, phones, etc.), and to secure adequate funding levels in the General Office Equipment/Technology Replacement Fund.

Revenues: The revenues for the General Office Equipment/Technology Replacement Fund, are from replacement charges (funded depreciation) applied against the operating funds of the Village via a transfer out that support the departments which utilize the subject equipment, surplus equipment sale proceeds, insurance claims, and investment income. The replacement charge (the transfer in) that will fund the General Office Equipment/Technology Replacement Fund is determined by the gross purchase price of the item divided by the anticipated life cycle, commonly referred to as the annual depreciation charges.

Trade-in or surplus sale values for the subject equipment are not included in the formula to help offset future cost increases in general office equipment and technology items that may be higher than the rate of inflation.

Income from the settlement of damage insurance claims on equipment, self insured or third party, resulting in the total loss of the village equipment shall be returned to the General Office Equipment/Technology Replacement Fund to enable the purchase of a replacement item.

Fund Balance: The reserve fund balance of the General Office Equipment/Technology Replacement Fund should be sufficient to meet the following objectives:
- Fund the current fiscal year equipment purchase needs;
- Include adequate resources for unanticipated replacement items not schedule in the current year, and;
- Generate sufficient investment income to offset inflation of the equipment replacement costs in conjunction with surplus sale revenue.
In Like Kind Replacement: The General Office Equipment/Technology Replacement Fund is structured to replace each piece of equipment by a unit of like kind. It is understood that capabilities and technology associated with the various pieces may change over the course of time. Cost increases due to upgrades, additions of options, or other improvements associated with items scheduled for replacement shall be highlighted as an element of the annual budget presentation, and shall either be funded from transfers from the operating funds or from unencumbered fund balance.

Annual Budget Detail: The annual fiscal year budget shall disclose the anticipated cost for the replacement of the equipment and the amount of money that is in the General Office Equipment/Technology Replacement Fund account for the replacement. In the event that the Fund account's resources are not sufficient to fully pay for the item(s), the difference and the means to make up the difference shall be noted in the budget document.

Additional to the Village's equipment inventory: These items shall be noted as “New Items” in the subject department’s fiscal year budget appropriation request. The new request, if approved, will be funded by future equivalent dollar amount transfer to the General Office Equipment/Technology Replacement Fund based on the replacement charge calculation.

Processes:
The process which will be used will consist of an on-line village-wide equipment inventory which tracks and dates each piece of equipment the village uses. This annually updated replacement plan will be the basis for planned expenditures.

Scheduled Replacement Guidelines:
Each piece of equipment shall be evaluated for replacement on an annual basis. Evaluation criteria shall include:
* The cost of maintenance per item;
* Age;
* General condition.

Each time a piece of equipment reaches its minimum useful life that piece of equipment would be eligible for replacement. This does not mean that equipment will automatically be replaced, only that it is eligible. However, in the event that a piece of equipment is problematic (major repair occurrence or when minor repairs outweigh the benefits of a new purchase) and has exceeded its useful life threshold, it will be replaced. This methodology benefits the village by getting the maximum use out of the purchased equipment.

This policy shall be subject to review by the FLAGG Committee as deemed appropriate. These standards are guidelines only and individual equipment life cycles may differ based on expected utilization or other operating conditions. In the event that management wishes to deviate from the guidelines, justifications shall be presented, including an understanding on how granting the deviation will affect the status of the General Office Equipment/Technology Replacement Fund. The replacement charges, i.e., depreciation amounts shall be adjusted as well to account for the change in timing for the replacement.

Any proposed deviation from the adopted guidelines shall be subject to the review and approval of the Finance Legal Administration General Government (FLAGG) Committee and entire Village Board.

Roles:
Information Technology:
* Prepares annual general office equipment/technology replacement plan with the Finance Department for the review and approval of the Village Manager’s Office and Village Board.
* Communicates information on the cost of operating technology equipment to the relevant Village departments.
* Provides leadership and coordination for the development of specifications for bids for the replacement of equipment, when necessary.
* Makes recommendations to the FLAGG Committee on the award of contracts for bids on replacement equipment.

Finance Department:
* Provides assistance to Information Technology on the development of the annual general office equipment/technology replacement plan.
Establishes depreciation schedules for all items in the General Office Equipment/Technology Replacement Fund.

Maintains the accounts for the General Office Equipment/Technology Replacement Fund.

Coordinates the bidding process associated with the replacement of equipment.

Other Village Departments:

Provides input to the team preparing the annual general office equipment/technology replacement plan, including whether deviations should be sought.

Provides input on the development of plans and specifications for the replacement equipment, when necessary.

Village Manager's Office:

Provides input and approval to the draft annual general office equipment/technology replacement plan prior to presentation to the Village Board.

Reviews and approves recommendations on the awards of bids for equipment.

Reviews requests for additional funding associated with the purchase of equipment where sufficient funds are not available in the General Office Equipment/Technology Replacement Fund.

Village Board - Finance Legal Administration and General Government Committee:

Reviews, modifies or approves the annual general office equipment/technology replacement plan.

Reviews, modifies, rejects or approves requests for additional funding associated with the purchase of equipment where sufficient funds are not available in the General Office Equipment/Technology Replacement Fund account.

Entire Village Board:

Reviews, modifies, rejects or accepts the FLAGG Committee's recommendations the general office equipment/technology replacement plan.

Reviews, modifies, rejects or accepts the FLAGG Committee's recommendations on requests for additional funding associated with the purchase of equipment where sufficient funds are not available in the General Office Equipment/Technology Replacement Fund.
Requests for New Computer Hardware, Parts, Peripherals and Networked Office Equipment
To provide guidelines for requesting new computer products or office equipment that is networked. Establishing guidelines will facilitate tracking new computer hardware, parts, peripherals and Networked office equipment. All these terms hardware, parts, etc., will be referred to as equipment in the Guidelines and Procedures.

Guidelines and Procedures
A. All new equipment requests will need to be made prior to budget formulation, usually in the October/November time frame.
B. New requests will be brought to the I.T. Department's attention and each request will have the endorsement from the requesting department's department head.
C. Every effort will be made by I.T. to understand the user department's request.
D. New hardware requests outside of the normal budget process will be handled on a case-by-case basis. The requesting department must have their department head's recommendation as part of the request.
Office Equipment / Technology Replacement

Goal: The Village of Schaumburg aspires to provide its employees with office equipment/technology equipment that enable them to offer effective and efficient services that our residents demand, while applying sound business approaches associated with: understanding the costs and benefits of office equipment/technology and its capabilities; funding purchases through the accumulation of resources as much as practical, and making decisions on replacements considering the level of usage, performance, and changing industry standards.

Expenditures: The General Office Equipment/Technology Replacement Fund shall be used to finance all office equipment/technology items which have met or exceeded their effective useful life as established by policy. Items that have exceeded established thresholds but which are still useful will be replaced upon the first major repair occurrence or when minor repairs outweigh the benefits of a new purchase. Replacement item's subject to financing through this policy shall include, but are not necessarily limited to, the following categories of equipment:
- Computer Central Processing Units (CPU's)
- Monitors
- Printers
- Copiers
- Audiovisual Equipment
- Telecommunications (phone/phone switches)
- 911 Emergency Dispatch Equipment (Communication Center Equipment)
- Other Office Equipment
- Other Communication Equipment

Funding: General Office Equipment/Technology Replacement Fund: The repository of the reserves for future office equipment/technology replacements is known as the General Office Equipment/Technology Replacement Fund. The purpose of the fund is to provide assured and adequate resources for the future replacement of office equipment and technology equipment, not subject to the financial constraints of the General Fund. Upon acquisition, any technology equipment with a purchase value in excess of $1,000.00, the village's threshold for tracking insurable equipment, or greater and an expected life in excess of one year shall be automatically included in the General Office Equipment/Technology Replacement Fund for future replacement, and the appropriate replacement charge will be collected from the fund from which the benefiting department derives its funding. The intent of the low threshold is to include all low cost equipment items that may have high volume quantities (computer monitors, phones, etc.), and to secure adequate funding levels in the General Office Equipment/Technology Replacement Fund.

Revenues: The revenues for the General Office Equipment/Technology Replacement Fund are from replacement charges (funded depreciation) applied against the operating funds of the Village via a transfer out that support the departments which utilize the subject equipment, surplus equipment sale proceeds, insurance claims, and investment income. The replacement charge (the transfer in) that will fund the General Office Equipment/Technology Replacement Fund is determined by the gross purchase price of the item divided by the anticipated life cycle, commonly referred to as the annual depreciation charges.

Trade-in or surplus sale values for the subject equipment are not included in the formula to help offset future cost increases in general office equipment and technology items that may be higher than the rate of inflation.

Income from the settlement of damage insurance claims on equipment, self insured or third party, resulting in the total loss of the village equipment shall be returned to the General Office Equipment/Technology Replacement Fund to enable the purchase of a replacement item.

Fund Balance: The reserve fund balance of the General Office Equipment/Technology Replacement Fund should be sufficient to meet the following objectives:
- Fund the current fiscal year equipment purchase needs;
- Include adequate resources for unanticipated replacement items not schedule in the current year, and;
- Generate sufficient investment income to offset inflation of the equipment replacement costs in conjunction with surplus sale revenue.

In Like-Kind Replacement: The General Office Equipment/Technology Replacement Fund is structured to replace each piece of equipment by a unit of like kind. It is understood that capabilities and technology associated with the various pieces may change over the course of time. Cost increases due to upgrades, additions of options, or other improvements associated with items scheduled for replacement shall be highlighted as an element of the annual budget presentation, and shall either be funded from transfers from the operating funds or from unencumbered fund balance.

Annual Budget Detail: The annual fiscal year budget shall disclose the anticipated cost for the replacement of the equipment and the amount of money that is in the General Office Equipment/Technology Replacement Fund account for the replacement. In the event that the Fund account’s resources are not sufficient to fully pay for the item(s), the difference and the means to make up the difference shall be noted in the budget document.

Additions to the Village’s equipment inventory: These items shall be noted as “New Items” in the subject department’s fiscal year budget appropriation request. The new request, if approved, will be funded by future equivalent dollar amount transfer to the General Office Equipment/Technology Replacement Fund based on the replacement charge calculation.

Processes:
The process which will be used will consist of an on-line village-wide equipment inventory which tracks and dates each piece of equipment the village uses. This annually updated replacement plan will be the basis for planned expenditures.

Scheduled Replacement Guidelines:
Each piece of equipment shall be evaluated for replacement on an annual basis. Evaluation criteria shall include:
* The cost of maintenance per item;
* Age;
* General condition.

Each time a piece of equipment reaches its minimum useful life that piece of equipment would be eligible for replacement. This does not mean that equipment will automatically be replaced; only that it is eligible. However, in the event that a piece of equipment is problematic (major repair occurrence or when minor repairs outweigh the benefits of a new purchase) and has exceeded its useful life threshold, it will be replaced. This methodology benefits the village by getting the maximum use out of the purchased equipment.

This policy shall be subject to review by the FLAGG Committee as deemed appropriate. These standards are guidelines only and individual equipment life cycles may differ based on expected utilization or other operating conditions. In the event that management wishes to deviate from the guidelines, justifications shall be presented, including an understanding on how granting the deviation will affect the status of the General Office Equipment/Technology Replacement Fund. The replacement charges, i.e., depreciation amounts shall be adjusted as well to account for the change in timing for the replacement.

Any proposed deviation from the adopted guidelines shall be subject to the review and approval of the Finance Legal Administration General Government (FLAGG) Committee and entire Village Board.

Unanticipated New Additions: Unless it can be shown to be in the interest of promoting the health, safety and welfare of the general public to do otherwise, all new requests for the purchase of additional pieces of equipment shall be presented to the Village Board as an element of the annual budget process.

Roles:
Information Technology:
* Prepares annual general office equipment/technology replacement plan with the Finance Department for the review and approval of the Village Manager’s Office and Village Board.
* Communicates information on the cost of operating technology equipment to the relevant Village departments.
* Provides leadership and coordination for the development of specifications for bids for the replacement of equipment, when necessary.
* Makes recommendations to the FLAGG Committee on the award of contracts for bids on replacement
equipment.
Finance Department:
* Provides assistance to Information Technology on the development of the annual general office
equipment/technology replacement plan.
* Establishes depreciation schedules for all items in the General Office Equipment/Technology
Replacement Fund.
* Maintains the accounts for the General Office Equipment/Technology Replacement Fund.
* Coordinates the bidding process associated with the replacement of equipment.
Other Village Departments:
* Provides input to the team preparing the annual general office equipment/technology replacement plan,
including whether deviations should be sought.
* Provides input on the development of plans and specifications for the replacement equipment, when
necessary.
Village Manager’s Office:
* Provides input and approval to the draft annual general office equipment/technology replacement plan
as part of the village budget presentation to the Village Board.
* Reviews and approves recommendations on the awards of bids for equipment.
* Reviews requests for additional funding associated with the purchase of equipment where sufficient
funds are not available in the General Office Equipment/Technology Replacement Fund.
Village Board - Finance Legal Administration and General Government Committee:
* Reviews, modifies or approves the general office equipment/technology replacement policy.
* Reviews, modifies, rejects or approves requests for additional funding associated with the purchase of
equipment where sufficient funds are not available in the General Office Equipment/Technology
Replacement Fund as submitted in the village budget.
Entire Village Board:
* Reviews, modifies, rejects or accepts the FLAGG Committee’s recommendations the general office
equipment/technology replacement plan as part of the overall village budget.
* Reviews, modifies, rejects or accepts the FLAGG Committee’s recommendations on requests for
additional funding associated with the purchase of equipment where sufficient funds are not available in
the General Office Equipment / Technology Replacement Fund.
Security Systems Policy

Purpose
To ensure that all computer systems within the Village that contain important or irreplaceable data are secure from damage due to tampering, vandalism or equally disturbing phenomenon. All departments utilizing the Village Network share common disk drives and therefore common data and programs which may be altered by all users of the Network. Security is required for all these systems regardless of the estimated value of the contents. Use will be regulated through the installation of an authorized security system compatible with such hardware and software.

Guidelines and Procedures
1. Individuals must comply with all stated policies and will be held accountable for their activities. Downloading data, software, or files downloaded from Internet into the Village’s network becomes Village property. Also, the Village does not permit the downloading of the following:
   - Personal software, images (to include downloaded screen savers), audio or videos;
   - Entertainment software, games or playing games on the Internet;
   - Streaming audio or video files; or
   - Downloading or distributing pirated software or data.
   Streaming audio and video is permitted for approved job-related training and educational events.
2. Stand-alone microcomputer systems will require security systems if the department determines that the data and programs contained within are confidential or valuable. Security systems will also be required if the department determines that the data contents are to be accessed by only certain individuals. If a computer has only public files and is not connected to the network, then it would be exempt from the required security systems.
3. Networks are required to have an authorized security system installed and active. Most networks that are available have adequate security built into them to meet Village requirements. Departments have the responsibility to determine which employees are to be considered authorized personnel. A list of the authorized individuals needs to be given to Information Technology for proper Network security set up. All access to the Network will be determined by the department head in consultation with the computer user representative. The result of a department allowing unqualified personnel to gain access to information of the Network areas such as the File Allocation Tables or to change programming defaults causing destruction, unwanted alterations or other damage is solely the responsibility of the departments. It is important that access to programming areas on the Network be available only to those deemed qualified.
4. It is the responsibility of Information Technology to ensure that all security systems are operable and up-to-date. All menu options, passwords, operators and automatic setup routines are to be monitored by Information Technology for completeness, accuracy and functionality.
5. All additions and deletions of users from the security systems must be done by Information Technology. Occasional changes in all user passwords may be implemented by Information Technology to prevent common knowledge of these keys. Those passwords will be changed at least once a year.
6. Additions or alterations in system menus due to additional programming options or other changes are the responsibility of Information Technology. All access will be maintained and monitored by Information Technology for completeness, accuracy and functionality.
7. All other computer systems within the Village must have an active security system.
Software Licenses Policy

Purpose
To ensure that all departments and Village personnel abide by the licensing agreements entered into with software manufacturers. To protect the rights of the individual software authors and to reduce the risk that the Village might impose on copyrights in daily operations.

Guidelines and Procedures
The Village and its employees will not infringe upon the copyrights of companies or individuals. Software must be properly licensed and registered and all agreed upon fees shall be paid for each license delivered. Employees are not to make copies other than those specified by the manufacturer.

Software shall not be brought from home and installed on a Village computer without written permission from the Director of Information Technology. Employees are not allowed to make copies of software for the purpose of home use unless the software is owned by the Village and written permission has been granted by the Director of Information Technology. This pertains, but is not limited to, software that was written by employees for the Village or software that was custom developed for the Village.

Any software developed by an employee during working hours or on Village equipment is considered the property of the Village and cannot be sold to or used by anyone for individual profit.

Ownership Policy
Any Village of Schaumburg employee or contractor who develops computer software (or other inventions) assigns all rights to that software or invention to the Village of Schaumburg if any one of the following is true:

a. it is developed using Village equipment and/or resources,

b. it is developed on Village-paid time,

c. it is copyrighted for the Village,

d. it incorporates or depends on Village information,

Any Village employee who develops computer software independent of the limitations (a - d) stated above, brings the software onto Village property, and uses it to support Village business thereby grants to the Village a permanent right to use and modify such software.

The employee may retain the right to market the software that is developed independent of the above limitations (a - d). However, marketing must not be done with Village equipment, supplies, facilities or time unless a written contract has been executed by the Village agreeing thereto. The Village will not accept any liabilities resulting from this marketing.

Any Village of Schaumburg employee who develops software independent of the limitations stated above may maintain rights of ownership from this software. These rights shall be subject to certain restrictions including but not limited to the following:

1. In this case, employees shall not sell programs to firms, businesses, companies, corporations, municipalities, etc., who perform services or supply products to the Village of Schaumburg.
2. Employees who develop and sell computer applications on their own time will not use Village time to consult with or help buyers of their application.
3. Employees may not sell programs or applications that are developed on Village computers, software, hardware, etc., unless there is a contractual agreement with the Village allowing such activity.

Municipalities or other public entities wishing to acquire applications developed by Village employees (in scope of his/her employment), may be provided copies of such applications pursuant to a license agreement with the Village and with written permission of the Director of Information Technology.

If other agencies or communities are interested in a software package that has been developed for the Village, the Director of Information Technology shall determine a fair price for compensation and a decision will be made by the Village Manager whether or not to distribute the software.

In some cases software developed for the Village will have specific license agreements that provide royalties to the Village in lieu of obtaining the actual title to the software. This arrangement is used when vendors wish to retain the rights to specific proprietary techniques used in custom applications code. Again, any sale of such custom software developed for the Village, but owned by the vendor must be approved by the Village Manager.
Software Standardization Policy

Purpose
To ensure long range, cost effective interdepartmental deployment of computer software. Software standards will be established, based on operational needs and consensus, to increase the benefits of sending and receiving interdepartmental data among Village of Schaumburg computer users. Providing software standards will assist in maximizing the compatibility of data exchanges between all Village computers; increase the effectiveness of training while minimizing software maintenance. Increased interdepartmental communications by means of software compatibility will assist employees in maintaining a high level of service to Village of Schaumburg residents.

Guidelines And Procedures
A. The Director of Information Technology is responsible for approving all software purchases within the Village of Schaumburg. Periodically, a list of software standards will be distributed by the Information Technology Department to all departments computer user representatives. Software standards will be based upon the following criteria:
   1. Program compatibility with existing hardware and software;
   2. Recommendations from the Information Technology Department and departmental computer user representatives following evaluation of a software package;
   3. Features and benefits that are applicable to the majority of departments;
   4. Availability of vendor support for the product;
   5. Cost/benefit analysis, if necessary;
   6. Ease of data file exchange for simplified data retrieval and transfers;
   7. Overall contribution to enhancing Village-wide computing and information processing.
B. Purchases and use of software version upgrades will be based upon the software standards criteria and approved by the Director of Information Technology.
C. Recommendations for additions and/or changes to the software standards list should be directed to the Director of Information Technology.
D. Documentation regarding department application of standardized software will be maintained by Information Technology. The information will be distributed upon request to departmental computer representatives.
E. The Information Technology Department will be responsible for distributing software standards information to department computer users.
F. Software packages are generally sold under a license agreement and may not be copied beyond the limits of that license agreement.
029 Village of Schaumburg, IL -- Telecommunications Policies and Procedures

Telecommunications Policies And Procedures

Voice Mail Usage

Purpose

To provide guidelines for the secure, effective and efficient use of the Voice Mail System. It sets forth the Village’s policy with regard to access to and proper use of voice mail messages sent or received by Village employees using the voice mail system. This system provides inter and intra departmental voice mail communications for authorized mailbox users.

Guidelines And Procedures

1. The voice mail system is a user friendly, privileged communications system that digitally creates, stores and forwards communications and data, from one user to one or more users throughout the Village.

2. Usage of the voice mail system: Voice mail is to be used as a last resort tool for recovering customer calls. It is not to be used as a substitute for employees answering the phone. All calls from our residents are to be answered first by an employee, and then by the voice mail system. Every attempt, whether departmentally or systematically, should be made to answer the call with a person. Voice mail is an option for the customer as a courtesy and as a backup to the employee’s call path. Failure on an employee’s part to answer their department’s call and abuse the voice mail system, could result in disciplinary action.

3. The Village reserves the right to monitor voice mail messages.

4. The Village reserves the right, with Village Manager approval, to access and disclose the contents of any employees voice mailbox. Such access may occur, but is not limited to, the Village’s need to investigate a possible violation of policy or a breach of the computer or voice mail system security. Any contents properly obtained under these guidelines, may be disclosed within and outside the Village without the consent of the employee, but only to those persons who have some reasonable need for access to the information.

5. Incidental and occasional personal messages will be permitted within the Village, but these messages will be treated the same as all other messages sent via the voice mail system.

6. Authorized users will be provided a voice mail box which allows for storage of that individual’s telephone voice mail. The user will access his/her voice mail box through the use of a voice mail box password/code. The confidentiality of this password will be the sole responsibility of each user. Any communications via the voice mail system will be attributed to the assigned name of the originating user.

7. No user shall divulge his/her mailbox password. Any person with knowledge of any password not his/her own, shall report this to his/her supervisor immediately. The supervisor will then take the appropriate steps for securing the mailbox.

8. No employee shall attempt any unauthorized access to the voice mail system. Any employee found to have engaged in unauthorized access of the system may be disciplined.

9. No employee shall use the voice mail system for mass distribution of personal or non-business information. These messages include, but are not limited to, those messages containing personal advertisements, personal opinions or personal requests.

10. Initial access for new users will be authorized and recommended by the employee’s department head and through their respective user group representative.

11. Initial training shall be provided by Information Technology or trained departmental staff, where possible.

12. The maintenance of the voice mail master list used on the system shall be Information Technology’s responsibility. Suggestions for changes should be forwarded to the employee’s respective user group representative for their recommendation.
Computer User Group Representatives Policy

Purpose
To establish an individual within each department who would be the responsible liaison for that department’s computer activities. The role of the computer representative is to support the effective and efficient use of computer systems within his or her department. This person acts as the conduit for all requests pertaining to the department’s computer systems and as the first line of defense in resolving computer related problems or issues.

Guidelines and Procedures
The computer representative will have a general working knowledge of his or her department’s computer systems. Each representative will be selected by his or her department head through consultation with the Director of Information Technology and is responsible for:

A. Assisting Information Technology with system security, menus and password assignments. All systems containing vital or valuable information must be protected against theft or destruction by a password system.
B. Requesting routine installation of software programs. This includes software not supported in general by the Village, but specific to the department. If the application is supported by an outside vendor then the representative is responsible for notifying Information Technology about the vendor and the application.
C. Assisting in basic computer problem resolution. If local problem resolution is not obtainable, the Information Technology Department should be contacted for additional help.
D. Distributing Village communications regarding current and future microcomputer/automation projects and training.
E. Attend monthly User Group meetings.
F. Providing Information Technology with vendor hardware service repair information following service calls, if necessary.
G. Notifying Information Technology of departmental hardware, software application needs, computer-related problem areas, and training needs.
Web Site Links
Purpose:
To provide basic guidelines as to which and what kind of entities may be allowed to have their web sites linked from the Village of Schaumburg web site.
Guidelines and Procedures:
A. Any entity requesting a link from the village’s web site must request the link by contacting the Village of Schaumburg Information Technology Department at which point the request will be evaluated to determine its acceptance.
B. The Information Technology Department will evaluate every request based on the following:
   1. The entity making the request is another government agency or educational institution that has a facility within the village and/or provides services to residents or businesses in Schaumburg.
   2. The entity making the request is one that the village is a member of, i.e., Convention and Visitor’s Bureau, Regional Coalition of Municipalities, Chamber of Commerce, etc.
   3. The entity making the request is noncommercial in nature and/or has a contractual agreement for the use of Village of Schaumburg facilities or is housed at a Village of Schaumburg facility.
   4. The entity making the request is a utility that serves the residents of the Village of Schaumburg.
   5. The entity making the request promotes tourism, industry, and economic welfare within Schaumburg. This would include links to sites maintained by organizations that have been identified by the village as sponsors of community events or festivals, i.e., Septemberfest, etc.
C. The review of requests will be conducted by the Information Technology Department and any “link” decisions will be made by the Director of Information Technology. In the event that requestor does not agree with the Director’s decision, that requestor may appeal to the Village Manager.
D. In all cases, the Village of Schaumburg will only allow links from its page that are consistent with the purpose of the village’s web site; to provide useful information and services to residents and businesses of Schaumburg and those who work with or share common membership in organizations with the village.
E. In the event that an outside party installs a Village of Schaumburg link on its site and that site is found to be objectionable and inappropriate (as defined by the Village’s Internet Acceptable Use Policy), the Village will seek to have the link removed by requesting this action, or if necessary, by taking appropriate legal action.
HIPAA Security
SUBJECT: Risk Analysis, Risk Management, Evaluation
PURPOSE
The purpose of this policy is to ensure Sedgwick County conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by Sedgwick County.

POLICY STATEMENT:
Sedgwick County shall conduct an accurate and thorough risk analysis to serve as the basis for Sedgwick County’s HIPAA Security Rule compliance efforts. Sedgwick County shall re-assess the security risks to its e-PHI and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business practices and technological advancements.

PROCEDURE:
1. The Security Officer shall be responsible for coordinating Sedgwick County’s risk analysis. The Security Officer shall identify appropriate Departmental Security Administrators within the organization to assist with the risk analysis.
2. The risk analysis shall proceed in the following manner:
   A. Document Sedgwick County’s current information systems.
      1. Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how organization’s information system network is configured. For example, see Table 1.
      2. Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.
   3. For each application identified, identify each licensee (i.e., authorized user) by job title and describe the manner in which authorization is granted.
   4. For each application identified:
      a. Describe the data associated with that application.
      b. Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.
      c. Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
      d. Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.
      e. Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident. For example, see Table 2.
   5. For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls. For example, see Table 3.
   B. Identify and document threats to the confidentiality, integrity, and availability (referred to as “threat agents”) of e-PHI created, received, maintained, or transmitted by Sedgwick County. Consider the following:
      1. Natural threats, e.g., earthquakes, storm damage.
      2. Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
      3. Human threats
         a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls.
         b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment.
c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail.
d. External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction.

D. Identify and document vulnerabilities in Sedgwick County’s information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to e- PHI, modification of e- PHI, denial of service, or repudiation (i.e., the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities. For example, see Table 4. In addition, consider taking the following additional steps:
1. Consider that security is an ongoing task, that the risks and vulnerabilities change over time, and that the organization needs to develop a proactive plan for determining appropriate resources (consultants, internal staff, hardware, software, vendors, etc.) to be utilized so that overall security and vulnerability objectives can be met.
2. Consider acquisition of an automated vulnerability scanning tool or use of a vendor or consultant who provides similar services. These automated systems identify security “holes” in networks, i.e., flaws in network design, lack of a current patch, or other ways viruses and other malicious software may be introduced.
3. Consider conducting a penetration test. Such a test involves an actual attempt to penetrate information systems. Identify freeware or shareware or purchase software to conduct such a test internally.
4. Consider retaining a consultant to perform security tests and evaluation of the tools deployed to help reduce vulnerability, whether software, hardware, or vendors. Such consultants typically will conduct or procure security assessments such as vulnerability scanning and penetration testing, will review administrative and physical controls, and can assist you in being proactive in terms of identifying and minimizing vulnerabilities.

E. Determine and document probability and criticality of identified risks. For example, see Table 4.
1. Assign probability level, i.e., likelihood of a security incident involving identified risk.
a. High (3) – Sedgwick County or similarly situated health care providers have experienced such an occurrence in the past; controls to eliminate the vulnerability are not considered effective.
b. Medium (2) – Sedgwick County or similarly situated health care providers previously have been alerted to the threat; such threat can be minimized with the adoption of reasonable safeguards; controls exist to reduce risk of such occurrence.
c. Low (1) – Neither Sedgwick County nor its peers have experienced an occurrence; controls exist that significantly reduce or eliminate risk of such occurrence.
2. Assign criticality level.
a. High (3) – death or serious injury; sentinel patient care event; inability to recover critical or sensitive data; high cost of recovery; major lawsuit; significant fines and penalties; loss of licensure or accreditation.
b. Medium (2) – physical injury/harm; complaint to government agency; significant cost of recovery; minor lawsuit; small fine or penalty; damage to reputation.
c. Low (1) – loss of productivity; nuisance; embarrassment; some data loss.
3. Determine risk score for each identified risk. Add together the probability score and criticality score. Those risks with a higher risk score require more immediate attention.

F. Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high-risk scores, as well as specific security measures and safeguards required by the Security Rule. For example, see Table 4.

G. Develop and document implementation strategy for critical security measures and safeguards.
1. Determine timeline for implementation.
2. Determine costs of such measures and safeguards and secure funding.
3. Assign responsibility for implementing specific measures and safeguards to appropriate person(s).
4. Make necessary adjustments based on implementation experiences.
5. Document actual completion dates.
6. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

3. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of e-PHI; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:

   A. Inspections, reviews, interviews, and analyses to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted) and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.

   B. Analysis to assess adequacy of controls within the network, operating systems, and applications. As appropriate, Sedgwick County shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvements.

The Security Officer shall be responsible for appropriately documenting such on-going evaluations.

Table 1:
Hardware/Software Inventory
Date Acquired
Location
Vendor
Licenses (software only)
Maintenance
Schedule
Hardware
Network devices
Workstations
Printers
Scanners
Mobile devices
Other
Operating system
Email application
Word Processing application
Scheduling application
Registration application
Billing application
Practice management application
Electronic Medical Record (EMR) application
Interfaces

Table 2:
Application and Data Criticality and Sensitivity
Application
Criticality (High- Medium-Low)
Data
Create/Receive/ Maintain/Transmit
Sensitivity (High-Medium- Low)

Table 3:
Information System Security Controls
Security Controls
Exists? (Y/N)
Describe Features of Controls
Policy and Procedure in Which Documented
Application:
Unique user identification
Access controls
Emergency access
Automatic logoff
Audit controls
Authentication
Data integrity
Encryption
Backup
Emergency operation plan
Disaster recovery plan

Table 4:
Risk Analysis and Management Form
Security Rule Requirement
Vulnerability
Potential Threat
Probability
Critically
Risk Score
Control (Date Implemented)

Administrative Safeguards
Security Management Functions –Information System Activity Review
Information Access Management/ Workforce Security –Authorization and/or Supervision
Information Access Management/
Workforce Security –Workforce Clearance Procedure
Information Access Management/
Workforce Security –Termination Procedures
Information Access Management/
Workforce Security –Access Authorization
Information Access Management/ Workforce Security –Access Establishment and Modification
Security Awareness and Training –Security Reminders
Security Awareness and Training –Protection From Malicious Software
Security Awareness and Training –Password Management
Security Incident Procedures –Response and Reporting
Contingency Plan –Data Backup Plan
Contingency Plan –Disaster Recovery and Emergency Mode Operation Plan
Contingency Plan –Testing and Revision Procedure
Physical Safeguards
Facility Access Controls –Facility Security Plan
Facility Access Controls –Access Control and Validation Procedures
Facility Access Controls –Maintenance Records
Workstation Use
Workstation Security
Device and Media Controls –Disposal
Device and Media Controls –Media Re-use
Device and Media Controls –Accountability
Device and Media Controls –Data Backup and Storage
Technical Safeguards
Access Control – Unique User Identification
Access Control – Emergency Access Procedure
Access Control – Automatic Logoff
Access Control – Encryption and Decryption
Audit Controls
Integrity – Mechanism to Authenticate e-PHI
Person or Entity Authentication
Transmission Security – Integrity Controls
Transmission Security - Encryption
SUBJECT: Information System Activity Review

PURPOSE
To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, system access, file access, security incidents, audit logs, and access reports.

POLICY STATEMENT:
Sedgwick County shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

PROCEDURE:
1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Sedgwick County’s information systems that contain or use e-PHI.
2. Each Departmental Security Administrator and DIO/IT Networking and Telecommunications shall be responsible for conducting reviews of Sedgwick County’s information systems’ activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
3. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer’s name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.
4. Such reviews shall be conducted annually or as required. Audits also shall be conducted if Sedgwick County has reason to suspect wrongdoing. In conducting these reviews, Departmental Security Administrators and DIO/IT Networking and Telecommunications shall examine audit logs for security-significant events including, but not limited to, the following:
   a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
   b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts; unauthorized access; and unauthorized file creation, modification, or deletion.
   c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
All significant findings shall be recorded using the report format referred to in Section 2 of this policy and procedure.
5. Departmental Security Administrators and DIO/IT Networking and Telecommunications staff shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to Sedgwick County’s administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy entitled Incident Response and Reporting.
HIPAA Security

SUBJECT: Information Access Management and Workforce Security

PURPOSE

The purpose of this policy is to ensure Sedgwick County authorizes access to e-PHI for its workforce members in a manner consistent with the HIPAA Privacy Rule, particularly the minimum necessary rule, and prevents unauthorized access to e-PHI by workforce members.

POLICY STATEMENT:

This policy reflects Sedgwick County’s commitment to ensure that all workforce members have appropriate authorization to access Sedgwick County’s information systems containing e-PHI as necessary to perform their job functions.

PROCEDURE:

Role-Based Access Rules

1. Departmental Security Administrators (DSAs) shall determine the appropriate level of access to hardware, applications, and data for each job position based on the need for such access to perform assigned job responsibilities. DSAs also shall determine what keys, tokens, and/or cards (if any) shall be furnished to persons in each job position. Such access rules shall be made using the principles of least privilege, need-to-know, and separation of duties. Supervisors/managers shall be responsible for furnishing necessary information to permit DSAs to determine appropriate access rules for each job position. If the duties, role, function, or responsibilities of a particular job position change, DSAs shall re-evaluate and make appropriate changes to the access rules for that job position. No change in the access rules for any job position shall be permitted without the express permission of DSAs. If new hardware, application, and/or data are introduced by Sedgwick County, DSAs shall make appropriate modifications to access rules for impacted job positions.

2. DSAs shall be responsible for maintaining a current list of access rules for each job position in the department. Any changes in access rules for any job position shall be properly recorded on such list. In addition, the DSA shall ensure that a written job description for each job title include the current access rules for that position.

Access Establishment and Modification

3. DSAs shall be responsible for establishing and modifying access privileges for each workforce member based on the access rules for his/her job position. DSAs also shall provide keys, tokens, and/or cards to each workforce member as provided in the access rules for his/her job position. No modification to a workforce member’s access privileges shall be made without a written request for such access from his/her supervisor. Upon hiring a new workforce member, such person’s supervisor or manager shall be responsible for requesting the appropriate level of access and keys, tokens, and/or cards for the new workforce member based on the applicable access rules for his/her job position. DSAs shall maintain a current master access list identifying the access granted and keys, tokens, and/or cards provided to each workforce member.

4. Every workforce member shall comply with the access rules for his/her job position. Any workforce member who attempts to gain access to e-PHI for which he/she does not have authorization or for purposes unrelated to his/her job responsibilities shall be subject to appropriate disciplinary action.

5. DSAs shall be responsible for conducting routine audits to determine whether workforce members’ actual access to hardware, applications, and data is consistent with established access rules for their job positions. Such audits shall be appropriately documented, and such documents shall be forwarded to and maintained by the Security Officer.

Access Termination

6. If a workforce member transfers to another job position, the workforce member’s existing supervisor or manager must ensure that existing access to hardware, applications, and data is terminated. The workforce member’s new supervisor or manager is responsible for requesting access consistent with the access rules for the new job position.
7. The DSA, in conjunction with the responsible supervisor/manager, shall be responsible for determining whether it is necessary to change locks and/or take other physical security measures at the facility following termination of a workforce member.

8. The Division of Human Resources shall retrieve from any terminated workforce member any keys, tokens, and/or cards provided to him/her by Sedgwick County. The Division of Human Resources shall immediately notify DIO/IT Networking & Telecommunications of the termination of employment for any workforce member and forward any returned keys, tokens, and/or cards to the proper Departmental Security Administrator. Upon receipt of such notice, DIO/IT Networking & Telecommunications and the affected DSA shall immediately revoke such former workforce member’s access to hardware, applications, and data. DSAs shall update the master access list to reflect such termination of access and return of keys, tokens, and/or cards.

9. The Security Officer shall be notified in the event keys, tokens, and/or cards are not collected from a terminated workforce member in a timely manner. The Security Officer shall determine whether additional steps shall be taken to address the security of the associated components (e.g., rooms, card reader controls, etc.).
035 Sedgwick County, KS – HIPAA Security Awareness and Training Policy

HIPAA Security
SUBJECT: Security Awareness and Training

PURPOSE
The purpose of this policy is to establish a security awareness and training program for all members of Sedgwick County’s workforce, including management.

POLICY STATEMENT:
All workforce members shall receive appropriate training concerning Sedgwick County’s security policies and procedures. Such training shall be provided prior to the effective date of the HIPAA Security Rule and on an ongoing basis.

PROCEDURE:

Security Training Program
1. The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of the HIPAA Security Rule and Sedgwick County’s security policies and procedures prior to April 21, 2005. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.

2. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of e-PHI, e.g., addition of new hardware or software, increased threats.

Security Reminders
3. The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.

4. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

Protection from Malicious Software
5. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
   a. Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail;
   b. The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current;
   c. Instructions to never download files from unknown or suspicious sources;
   d. Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software;
   e. The importance of backing up critical data on a regular basis and storing the data in a safe place;
   f. Damage caused by viruses and worms; and
   g. What to do if a virus or worm is detected.

Password Management
6. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:
   a. Passwords must be changed every 90 days.
b. A user cannot reuse a password.
c. Passwords must be at least seven digits and contain three of the following four types of characters:
   1) Upper case alphabetic characters,
   2) Lower case alphabetic characters,
   3) Numeric characters, and
   4) Special characters (e.g., &, #, @).
d. Commonly used words, names, initials, birthdays, addresses, social security numbers, or phone numbers cannot be used as passwords.
e. A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.
f. Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.
g. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
h. Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
i. Any employee who is directed by the Security Officer to change his/her password to conform with the aforementioned standards shall do so immediately.
HIPAA Security
SUBJECT: Security Incident Reporting and Response

PURPOSE
The purpose of this policy is to establish appropriate procedures to identify security incidents, procedures to report those incidents, and procedures to respond to incidents.

POLICY STATEMENT:
This policy covers the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, the documentation of security incidents and their outcomes, and the evaluation of security incidents as part of ongoing risk analysis and risk management.

DEFINITION:
A security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Examples of security incidents include the following: property theft (hardware or software); compromised passwords, tokens, or other means of controlled access to e PHI; lost access badge; unauthorized access; unauthorized use of accounts or privileges; malicious code or virus; hacking (actual or attempted); identity theft; electrical power outages; hardware failures; human error; and acts of God (e.g., tornados, fire, earthquake, and hurricanes).

PROCEDURE:
1. An employee suspecting a security incident shall immediately notify the Security Officer by telephone or in person. To the fullest extent possible, such employee shall furnish the date and time of the incident and the circumstances surrounding the event. Such reports shall be treated as confidential information.
2. The Security Officer shall take immediate action to minimize the impact of any security incident and conduct an investigation concerning the cause of the incident. Such action may include the following:
   a. Identify all assets potentially compromised by the incident.
   b. Disconnect the affected component(s) from the network without removing power to the component(s).
   c. Ensure that all evidence (e.g., disks) is sealed in secure containers, and that access is controlled to these containers.
   d. Back up the compromised machine to unused media (for evidence retention purposes), controlling such evidence as noted above; make additional, separate backups for investigation and/or restoration purposes.
   e. Change passwords used on affected systems and/or networks as necessary.
   f. Restore affected systems using the last uncompromised backup.
   g. Interview employees with knowledge concerning the incident and impacted assets.
   h. Identify any exploited vulnerabilities as causes of the incident.
   i. Identify any damage/loss caused by the incident.
   j. Identify and implement remedial measures to restore/repair any damage/loss caused by the incident.
   k. If appropriate, impose or recommend discipline on involved employees.
3. The Security Officer shall generate a written report concerning each detected security incident. Such report should include the following information:
   a. Description of incident
   b. Date of incident
   c. Time incident was identified
   d. Person who identified the incident
   e. How the incident was identified
   f. Damage caused
   g. Employee(s) involved
h. Description of Security Officer’s investigation
i. Summary of the results of the investigation including cause of incident, if known
j. Date investigation initiated and date investigation completed
k. Remedial action proposed
l. Remedial action implemented and date of implementation
m. Personnel action taken

4. All security incident reports shall be reviewed as part of Sedgwick County’s ongoing risk analysis and appropriate proactive measures shall be taken as part of Sedgwick County’s risk management plan to prevent the future occurrence of a similar incident.
HIPAA Security
SUBJECT: Contingency Plan
PURPOSE
The purpose of this policy is to establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain e-PHI.

POLICY STATEMENT:
Sedgwick County is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing e-PHI. Sedgwick County shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

PROCEDURE:
Data Back-up Plan
1. Sedgwick County, under the direction of the Security Officer, shall develop and implement a data back-up plan to create and maintain retrievable exact copies of e-PHI.
2. The Security Officer shall be responsible for developing written back-up procedures for data relating to each application identified in the inventory generated as part of Sedgwick County’s risk analysis, as well as the operating system and application files. Such procedures shall identify the server or personal computer on which the data is maintained; the person responsible for the back-up; the frequency with which the back-up shall be performed, including incremental and full back-ups; whether the back-up is to be performed manually or automatically; the media on which the back-up will be maintained; the location at which the back-up shall be stored; and the period of time the back-up will be maintained. Back-ups shall be stored either off-site or on-site in a fireproof locked vault or secure cabinet. Back-ups shall be password protected. The Security Officer shall review and update such back-up procedures as necessary.
3. The Security Officer shall monitor storage and removal of back-ups and ensure all applicable access controls are enforced.
4. The Security Officer shall identify critical files to be printed on a periodic basis with the hard copies stored in a secure location, and shall develop and implement appropriate procedures relating to the generation and maintenance of such hard copies.
5. The Security Officer shall test back-up procedures on a quarterly basis to ensure that exact copies of e-PHI can be retrieved and made available. The Security Officer shall document such testing. To the extent such testing indicates need for improvement in back-up procedures, the Security Officer shall identify and implement such improvements in a timely manner.

Disaster Recovery and Emergency Mode Operations Plan
1. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of (a) restoring or recovering any loss of e-PHI and/or systems necessary to make e-PHI available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and (b) continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which back-ups are stored or other secure off-site location.
2. The disaster recovery and emergency mode operation plan shall include the following:
   b. Current copy of the written back-up procedures developed and updated pursuant to this policy.
   c. An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions with patients.
d. Identification of emergency response teams. Members of such teams shall be responsible for the following:

1. Determining the impact of a disaster and/or system unavailability on Sedgwick County's operations.
2. In the event of a disaster, securing the site and providing ongoing physical security.
3. Retrieving lost data.
4. Identifying and implementing appropriate “work-arounds” during such time information systems are unavailable.
5. Taking such steps necessary to restore operations.

e. Procedures for responding to loss of electronic data including, but not limited to, retrieval and loading of back-up data or methods for re-creating data should back-up data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of Sedgwick County’s risk analysis. (See policy entitled Security Management Process – Risk Analysis, Risk Management, and Evaluation.)

f. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:

1. Members of the immediate response team.
2. Facilities at which back-up data is stored.
3. Information systems vendors.
4. All current workforce members.

3. The disaster recovery team shall meet on at least a semi-annual basis to (a) review the effectiveness of the plan in responding to any disaster or emergency experienced by Sedgwick County; (b) in the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and (c) review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.
HIPAA Security
SUBJECT: Business Associates
PURPOSE
The purpose of this policy is to ensure Sedgwick County amends its business associate agreements with those business associates that create, receive, maintain, or transmit e-PHI on behalf of Sedgwick County.

POLICY STATEMENT:
Sedgwick County shall not permit a business associate to create, receive, maintain, or transmit e-PHI on behalf of Sedgwick County after April 21, 2005, unless the business associate has executed an amendment to its business associate agreement with Sedgwick County relating to the security of e-PHI.

PROCEDURE:
1. The Security Officer, with the assistance of the Privacy Officer, shall identify all business associates that create, receive, maintain, or transmit e-PHI on behalf of Sedgwick County.
2. By no later than March 1, 2005, the Security Officer shall forward to such business associates an amendment to the business associate agreement relating to the security of e-PHI. Such amendment shall include the following language:
   “Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the e-PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity, as required by the Security Rule. Business Associate shall ensure that any agent, including a subcontractor, to whom Business Associate provides such information agrees to implement reasonable and appropriate safeguards to protect it.”
3. The Security Officer shall monitor the return of executed amendments from business associates. Such amendments shall be filed with the original business associate agreements.
4. If any identified business associate fails to return an executed amendment by April 21, 2005, Sedgwick County shall not permit such business associate to create, receive, maintain, or transmit e-PHI on behalf of Sedgwick County until the business associate executes such an amendment.
5. Sedgwick County may enter into an amendment drafted by a business associate provided such amendment is substantially similar to the amendment proposed by Sedgwick County.
6. Sedgwick County’s standard business associate agreement shall be revised to include a provision with language substantially similar to that contained in the aforementioned amendment. Such revised business associate agreement shall be utilized with all business associates with which Sedgwick County enters into a relationship following the effective date of this policy.
7. If any member of Sedgwick County’s workforce has reason to believe a business associate has violated the terms of a business associate agreement relating to e-PHI, such person shall report such information to the Security Officer as soon as possible. The Security Officer shall investigate the matter and take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or arrangement is not feasible, the Security Officer shall report the problem in writing to the Secretary of the U.S. Department of Health and Human Services. Such communication shall contain a description of the breach and the reasons why termination of the relationship between the parties is not a viable alternative.
HIPAA Security

SUBJECT: Facility Access Controls

PURPOSE

The purpose of this policy is to ensure Sedgwick County’s HIPAA-impacted departments adopt and maintain appropriate physical measures to limit physical access to its electronic information systems and the facility in which they are housed while ensuring that properly authorized access is allowed.

POLICY STATEMENT:

Sedgwick County’s HIPAA-impacted departments shall develop, implement, and regularly update a facility security plan and access controls and validation procedures, and maintain maintenance records for the physical components of the facility relating to security.

DEFINITION:

“Facility” refers to the department’s physical premises, including interior and exterior of any building in which the department’s operations are located, including the building’s construction, design, landscaping, fire protection, electrical wiring, etc.; access points (such as doors, windows), and other means by which people or information may enter or exit; and equipment and media contained within the building.

PROCEDURE:

Facility Security Plan/Access Control and Validation Procedures

1. The Departmental Security Administrator (DSA) shall be responsible for developing, implementing, and regularly updating the facility security plan. Such plan shall identify those validation procedures and environmental and access controls currently utilized by Sedgwick County.

2. The Facility Security Plan shall include procedures for validating the identity of those persons physically present at the facility. Such procedures shall address the following:
   - Identification badges for workforce members.
   - Patient escorts.
   - Visitor sign-in sheets, badges.
   - Visitor escorts.

3. In identifying reasonable and appropriate environmental and access controls to be included in the department’s Facility Security Plan, the DSA shall (a) review the results of the risk analysis to identify critical threats to the department’s information systems that may be addressed by one or more of the following environmental and access controls; (b) consider whether the control places unacceptable restrictions on the department’s operations; and (c) consider the costs associated with the control against the level of security gained by its implementation.

   Environmental controls:
   - Fire alarms and smoke detectors
   - Fire suppression equipment (sprinklers, fire extinguishers)
   - Equipment for handling biohazards (clothing, gear, etc.)
   - Water detection alarms
   - Power strips with surge protectors
   - Power conditioners
   - Multiple power feeds
   - Uninterruptible power supplies
   - Back-up generators
   - HVAC controls to protect computer equipment
   - Heat sensors for computer equipment
   - Humidity controls
   - Air filtering systems

   Access controls:
   - Appropriate locks on facility access doors (key, combination lock, swipe badges, proximity cards)
   - Isolate critical equipment, sensitive files, etc., in restricted access areas
   - Signage identifying restricted areas
   - Appropriate locks on restricted access areas
   - Surveillance cameras, alarms, motion detectors
- Property control tags or engraving to establish proof of ownership for equipment
- Panic buttons for immediate communication with security/police
- Private security service to patrol facility
- Alarmed emergency exit doors
- Locked file cabinets
- “Clean desk” policy

5. The departmental Facility Security Plan shall include the facility layout developed as part of the risk analysis showing location of all information systems equipment, power sources, telephone jacks and other telecommunications equipment, network access points, and environmental and access controls.

6. A copy of the department’s Facility Security Plan shall be accessible to all workforce members. All workforce members shall receive training concerning the relevant portions of the Facility Security Plan. Employees shall be subject to disciplinary action for failure to adhere to the relevant requirements of the Facility Security Plan.

7. The DSA shall regularly review and update the Facility Security Plan.

Maintenance Records
1. The DSA must approve any maintenance, repairs, or modifications to the physical security components of the facility including locks, doors, and other physical access control hardware prior to the commencement of work.
2. The DSA must inspect and approve any maintenance, repair, or modification prior to the completion of work.
3. If any third party is granted special access to the facility for purpose of performing maintenance, repairs, or modifications (e.g., key, access code), the DSA shall be responsible for revoking such access immediately upon completion of the work.
4. The DSA shall be responsible for maintaining documentation of all maintenance, repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware. Such documentation shall include the following information:
   - Clear definition of the reason(s) for the repair/modification;
   - The nature of what was repaired/modified;
   - The name of the organization engaged to perform the repair/modification;
   - The technician(s) who performed the repair/modification;
   - The date(s) the work was performed;
   - The date completed;
   - The cost and purchase order number under which the work was performed.
HIPAA Security
SUBJECT: Workstation Use and Security
PURPOSE
The purpose of this policy is to specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access e-PHI. The policy also identifies physical safeguards for all workstations that access e-PHI to restrict access to authorized users.

POLICY STATEMENT:
Sedgwick County shall maintain appropriate procedures and safeguards to ensure members of the workforce utilize its workstations in an appropriate and secure manner.

DEFINITION:
“Workstation” refers to any screen or other computer device used to create, receive, maintain, or transmit e-PHI. This includes, but is not limited to, “dumb terminals”; “thin clients”; desktop, laptop and notebook computers; tablets; PDAs; Blackberrys; and remote computers connected by VPN.

PROCEDURE:
1. Workforce members shall be given access and authorization to use Sedgwick County’s information systems in a manner consistent with the policy entitled “Information Access Management and Workforce Security.” An appropriate access control system shall be installed on all workstations. Workstations shall be configured to require a user to enter a unique user ID and password to gain access. Sedgwick County may remove or deactivate any workforce member’s user privileges when necessary to preserve the integrity, confidentiality, and availability of its facilities, user services, and data.
2. Workforce members shall use workstations for Sedgwick County’s business purposes. Highly limited, reasonable personal use of workstations is permitted; however, a workforce member should assume that any information created, received, maintained, or transmitted is not private. Sedgwick County reserves the right to periodically access, monitor, print, copy, and disclose the contents of computer files and drives and e-mail messages.
3. Workforce members shall not download files from unknown or suspicious sources, nor open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source.
4. Workforce members shall not use any workstation to send any message or download or retrieve any materials (video or audio) that could be considered inappropriate or illegal under state or federal law. Workstations shall not be used to store or transmit messages or materials (video or audio) having language or images that may reasonably be considered offensive, harassing, demeaning, or disruptive to any member of the workforce. Such prohibited conduct includes, but is not limited to, sexually explicit or derogatory comments or images, gender-specific comments, racial epithets and slurs, or any comments, jokes, or images that would offend someone or create a hostile work environment based on his/her race, color, sex, religion, creed, national origin, age, or disability. Workforce members are prohibited from sending or receiving messages or materials on workstations in a way which includes the use of profane or offensive language or, in the judgment of management, is determined to be profane, demeaning, insulting, disruptive, threatening, intimidating, violent, defamatory, harassing, embarrassing, insubordinate, or otherwise inappropriate or unprofessional.
5. Only approved software may be loaded on any workstation. Members of the workforce are prohibited from downloading any software to a workstation without the express permission from the Chief Technology Officer (CTO).
6. Password protected screen savers shall be installed on all workstations so that when a user is away from their computer, unauthorized persons do not gain access to such workstation or confidential information. Such password protected screen savers shall be configured to activate after a short interval (and shall also be capable of being manually activated by a user) so that after such screen saver activates, the computer screen thereafter does not display any confidential information and the computer itself cannot be utilized again until a password is entered. The length of time before a screen saver
activates shall be set to avoid disclosure of confidential information to unauthorized persons, as could happen if a user left their work area and forgot to manually activate the screen saver.

7. Laptop and notebook computers, PDAs, and other mobile devices shall have power-on passwords or data encryption to reduce the likelihood of data access or compromise should such device be lost or stolen.

8. Software to detect malicious software shall be installed on all workstations. DIO/IT Networking & Telecommunications shall be responsible for acquiring such software for Sedgwick County and any necessary subscriptions to receive virus signature updates. DIO/IT Customer Support Technicians shall be responsible for installing and configuring the software, and ensuring that the virus signature files are updated on a regular basis. Any available “auto-protect” features will be enabled, full alerts set, logging functions turned on, and quarantine and repair options will be selected.

9. Upon detection of malicious software, Sedgwick County shall take steps to prevent further infection. Users shall cease using workstations until the situation is resolved. They should not attempt to send or receive e-mails, open new programs, or reboot computers. Once the software has been contained and quarantined, DIO/IT Customer Support Technicians shall clean/repair any infected files.

10. Workstation monitors shall be positioned so that they cannot be easily seen by anyone other than the user. In high-traffic areas, workstations shall be located behind enclosures or partitions that shield the view of the information displayed.

11. When leaving a workstation or other computer system unattended, workforce members must lock or activate the automatic logoff mechanisms (e.g. Ctrl-Alt-Delete and Lock Computer) or lock out of all applications and database systems containing e-PHI. Workforce members shall log-off workstations prior to the completion of their workday.
HIPAA SECURITY
SUBJECT: Device and Media Controls
PURPOSE
The purpose of this policy is to protect e-PHI as it is received into and removed from Sedgwick County’s facilities.

POLICY STATEMENT:
Sedgwick County shall appropriately dispose of or re-use media and track the receipt and removal of hardware and electronic media.

PROCEDURE:
Disposal
1. When media is worn, damaged, or otherwise no longer required, it shall be disposed of in a secure manner. Magnetic media such as hard drives, floppy disks, and backup tapes should be rendered completely unusable prior to their disposal. The media should be degaussed, or physically damaged beyond repair. The precise mechanism will be dictated by the nature of the device being decommissioned.
2. Surplus equipment shall be routed to DIO/IT for proper disposal. The Security Officer shall be responsible for maintaining a log of such disposal.

Media Re-Use
1. Sedgwick County shall not re-sell or donate computers or media to any workforce member or third party, with the exception of computers from which the hard drive has been removed, destroyed, and replaced; or the data overwritten by products compliant with US Department of Defense 5220.22 M standards.
2. Prior to making removable media available for reuse within the organization (e.g., relocating workstations or servers), all e-PHI and software utilized to access e-PHI must be permanently deleted or overwritten by products to US Department of Defense 5220.22 M compliant standards.

Accountability
1. The Departmental Security Administrator shall regularly update the information systems inventory generated as part of Sedgwick County’s risk analysis by adding any new hardware or software acquired by Sedgwick County and deleting any hardware or software no longer utilized by Sedgwick County.
2. The Departmental Security Administrator shall regularly update the list of licensees for the various applications utilized by Sedgwick County generated as part of Sedgwick County’s risk analysis to reflect personnel changes within the organization.
3. The Departmental Security Administrator must approve any removal of hardware and/or software from the facility. The Departmental Security Administrator will assess the reason(s) for a given request, and make a decision that considers the requester’s access and clearance levels, job requirements, sensitivity of the components, period/frequency of removal, and any applicable policies and Business Associate agreements. Upon return to the facility, the equipment will be inspected to the degree necessary by the Departmental Security Administrator.
HIPAA Security

SUBJECT: Access Controls

PURPOSE

The purpose of this policy is to ensure that Sedgwick County maintains an appropriate level of access controls proportionate to the sensitivity and criticality of networks, systems, and applications that contain electronic protected health information ("e-PHI").

POLICY STATEMENT:

Sedgwick County is committed to implementing technical safeguards for information systems that maintain e-PHI to allow access only to those persons or software programs that have been granted access rights.

PROCEDURE:

Access Controls

1. Departmental Security Administrators shall configure access controls on all applications using e-PHI to regulate access based on approved authorizations developed in accordance with the policy entitled Information Access Management and Workforce Security.

2. Departmental Security Administrators shall configure system auditing to record all access control setting modifications.

3. Departmental Security Administrators shall verify that access permissions are set correctly and functioning properly when any modifications are made to approved authorizations.

4. Every year, Departmental Security Administrators shall review access permissions to ensure they are set correctly and functioning properly. Departmental Security Administrators shall document the results of such review and take appropriate remedial measures to correct any inappropriate or inaccurate access permissions.

5. Only Departmental Security Administrators shall have authority to create or change a workforce member's access control settings. Departmental Security Administrators shall make such modifications only upon receipt of written permission from the workforce member's supervisor.

Unique User Identification

1. DIO/IT Networking & Telecommunications shall assign unique user identification (user ID) to each workforce member for purposes of identifying and tracking user identity. DIO/IT Networking & Telecommunications shall maintain a record of user name assignments in a secure location.

2. Each workforce member's unique user identification shall be based on his/her first initial and last name. For example, if the user's name is Theresa Jones, her unique user ID would be “tjones.” Duplicate user identification shall be eliminated by inserting a middle initial or a sequential number as needed (e.g., tjones, tajones, t1jones, etc.).

3. Generic or shared user IDs shall not be utilized under any circumstances.

Emergency Access Procedure

1. Any situation in which a delay in accessing vital information could create imminent medical danger to a patient provides reason to utilize emergency access procedures. Such procedures permit an individual to access information for which he/she otherwise would not have authorization to access.

2. Sedgwick County shall work collaboratively with its IT vendors to establish appropriate emergency access procedures to override usual access controls.

3. Departmental Security Administrators shall regularly test emergency access procedures to ensure the appropriate levels of availability and restrictions exist.

Automatic Logoff

1. Applications and databases using e-PHI shall employ inactivity timers or automatic session logoff mechanisms.

2. To prevent unauthorized access to e-PHI, password-protected screensavers shall be installed on all workstations. Such screensavers shall be set to activate after the workstation has been unused for five minutes. To restart a session following a period of inactivity, the user must re-enter the password (and/or other authentication mechanism as required) when prompted.

3. Departmental Security Administrators shall periodically inspect workstations to ensure password-protected screensavers are functioning properly.
Encryption and Decryption
1. To the extent Sedgwick County’s risk analysis indicates a need to protect data at rest, Sedgwick County shall use encryption as a method of denying access to information in a file.
2. The Security Officer shall determine the workforce members requiring encryption/decryption capabilities, based on approved authorizations developed in accordance with the policy entitled Information Access Management and Workforce Security.
3. Based on vendor’s instructions, Security Officer shall generate encryption keys and/or certificates for each pertinent workforce member.
4. Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA shall be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Sedgwick County’s key length requirements shall be reviewed regularly and updated as technology allows.
5. The Security Officer shall authenticate each workforce member (e.g., by face-to-face inspection of a valid photo ID) prior to issuing any key.
6. Encryption keys shall be changed for each user every year. Keys shall be revoked upon termination, change in job responsibilities, or as a result of non-compliance.
HIPAA Security

SUBJECT: Audit Controls

PURPOSE

The purpose of this policy is to ensure that Sedgwick County implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information (“e-PHI”).

POLICY STATEMENT:

Sedgwick County is committed to routinely auditing users’ activities in order to continually assess potential risks and vulnerabilities to e-PHI in its possession. As such, Sedgwick County will continually assess potential risks and vulnerabilities to e-PHI in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

DEFINITIONS:

Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

PROCEDURE:

1. See policy entitled “Information System Activity Review” for the administrative safeguards for auditing system activities.

2. Departmental Security Administrators shall enable event auditing on all computers that process, transmit, and/or store e-PHI for purposes of generating audit logs. Each audit log shall include, at a minimum, user ID, login time and date, and scope of patient data being accessed, for each attempted access. Where possible, audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.

3. Sedgwick County shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.
HIPAA Security
SUBJECT: ePHI Integrity
PURPOSE
The purpose of this policy is to protect Sedgwick County’s e-PHI from improper alteration or destruction.

POLICY STATEMENT:
Sedgwick County shall implement and maintain appropriate electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner.

PROCEDURE:
1. To the fullest extent possible, Sedgwick County shall utilize applications with built-in intelligence that automatically checks for human errors.
2. Sedgwick County shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.
3. To prevent transmission errors as data passes from one computer to another, Sedgwick County will use encryption, as determined to be appropriate, to preserve the integrity of data.
4. Sedgwick County will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.
5. To prevent programming or software bugs, Sedgwick County will test its information systems for accuracy and functionality before it starts to use them. Sedgwick County will update its systems when IT vendors release fixes to address known bugs or problems.
6. Sedgwick County will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
7. Workforce members shall keep magnetic media away from strong magnetic fields and heat. (For example, computers should not be left in automobiles during the summer months.)
HIPAA SECURITY
SUBJECT: Person or Entity Authentication
PURPOSE
The purpose of this policy is to establish procedures to verify that the person or entity seeking access to e-PHI is the one claimed.
POLICY STATEMENT:
Sedgwick County is committed to maintaining formal procedures to verify that an individual or entity seeking access to e-PHI is the one claimed.
PROCEDURE:
1. DIO/IT shall configure information systems to enforce the rules relating to password usage found in the policy entitled Security Awareness and Training. DIO/IT staff shall conduct initial and follow-up tests to confirm the proper functionality of this authentication mechanism.
2. DIO/IT Security shall routinely run a password-cracking program for purposes of identifying users with weak or non-conforming passwords. Security staff shall promptly report such findings to the Security Officer.
3. Access to password files shall be limited to a “least privilege” and “need-to-know” basis and the contents of such file shall be encrypted.
SUBJECT: Transmission Security Controls

PURPOSE

The purpose of this policy is to implement technical security measures to guard against unauthorized access to e-PHI transmitted over any electronic communications network, including the Internet, leased lines, dial-up lines, private networks, and telephone voice response and “faxback” systems.

POLICY STATEMENT:

Sedgwick County shall adopt reasonable technical safeguards to protect the confidentiality, integrity, and availability of e-PHI transmitted over any electronic communications network.

PROCEDURE:

Integrity Controls

1. Sedgwick County shall maintain adequate firewalls to protect its networks. Firewalls shall be configured to “deny” rather than “allow” as their default policy. Any unused firewall port shall be closed unless the Chief Technology Officer confirms in writing the need to keep the port open. DIO/IT Systems & Security shall be responsible for properly maintaining and updating firewalls. DIO/IT Systems & Security staff shall examine firewall audit trails daily and reevaluate the security configuration of firewalls periodically.

2. Sedgwick County shall adopt a message authentication tool to ensure data that are transmitted are the same data that are received. Such tool shall be equivalent to or compatible with the message authentication features employed by entities with which Sedgwick County communicates. Such tools include Message Authentication Codes (“MAC”), which are built upon message digest (e.g., MD5 or SHA) and encryption methods.

3. Determine the information communicated across networks for which data integrity will be checked; ensure that all traffic containing e-PHI is included.

Encryption

1. To the extent Sedgwick County’s risk analysis reveals a need to protect e-PHI transmitted over the Internet, Sedgwick County shall adopt procedures for encrypting such transmissions.
047 Sedgwick County, KS – HIPAA Security Officer Job Description

SEDGWICK COUNTY SECURITY OFFICER JOB DESCRIPTION
Position Title: Security Officer
Immediate Supervisor: Chief Technology Officer
General Purpose: The Security Officer is responsible for developing and monitoring practices to ensure that Sedgwick County’s e-PHI is secure from unauthorized access, protected from inappropriate alteration, physically secure, and available to authorized users in a timely fashion.
Responsibilities:
* Develops and maintains thorough working knowledge of federal and state laws and regulations concerning the security of e-PHI.
* Oversees the development, management approval, implementation, and maintenance of relevant policies and procedures.
* Understands and works with technical staff, vendors, and consultants to develop and maintain security technology.
* Understands and works with staff responsible for physical security, including security consultants and vendors.
* Handles third-party inquiries concerning Sedgwick County’s security practices.
* Performs initial and periodic risk assessments and ongoing compliance monitoring activities.
* Oversees security training for members of Sedgwick County’s workforce and other appropriate third parties and ensures compliance through periodic security audits.
* Receives reports of security breaches, takes appropriate action to minimize harm, investigates breaches, and makes recommendations to management for sanctions.
* Participates in the development, implementation, and ongoing compliance monitoring of all business associate agreements.
* Works cooperatively with other employees to ensure compliance with security practices by all workforce members and consistent application of sanctions for failure to comply with such practices.
* Establishes and administers a process for receiving, documenting, investigating, and responding to all complaints concerning Sedgwick County’s security practices.
* Coordinates activities to foster security awareness within Sedgwick County.
* Revises the security program as necessary to comply with changes in the law, regulations, professional ethics, and accreditation requirements.
Qualifications:
* Demonstrate familiarity with the legal requirements relating to the HIPAA Security Rule, as well as the ability to communicate effectively with and coordinate the efforts of technical and non-technical personnel.
* Knowledge in and the ability to apply the principles of project management and change management.
* Familiarity with all aspects of Sedgwick County’s operations, especially those relating to the security of e-PHI.
* Demonstrates organization, facilitation, communication, and presentation skills.
Access to Protected Health Information:
The Security Officer shall have access to all media containing e-PHI for the purpose of monitoring and auditing compliance with information security laws and Sedgwick County’s internal policies and procedures relating to e-PHI and investigating and responding to complaints concerning Sedgwick County’s security.
SEDGWICK COUNTY DEPARTMENTAL SECURITY ADMINISTRATOR TASKS
Position Title: Departmental Security Administrator        Immediate Supervisor: Varies
General Purpose: The Departmental Security Administrator (DSA) is responsible for developing and
monitoring practices to ensure that their department’s e-PHI is secure from unauthorized access,
protected from inappropriate alteration, physically secure, and available to authorized users in a timely
fashion.
Responsibilities:
* Develops and maintains a basic understanding of federal and state laws and regulations concerning the
security of e-PHI.
* Understands and works with DIO/IT technical staff, departmental staff, and the Security Officer to
develop and maintain security technology.
* Understands and works with staff responsible for physical security, including security consultants and
vendors.
* Handles departmental inquiries concerning Sedgwick County’s security practices.
* Assists in performing initial and periodic risk assessments and ongoing compliance monitoring activities.
* Receives notifications of security breaches, assists in taking appropriate action to minimize harm,
assists in investigating breaches, and makes recommendations to Security Officer for sanctions.
* Participates in the development, implementation, and ongoing compliance monitoring of all business
associate agreements.
* Works cooperatively with other departmental employees to ensure compliance with security practices by
all department workforce members.
* Forwards notification of any complaints concerning Sedgwick County’s security practices to the Security
Officer.
* Encourages activities to foster security awareness within Sedgwick County.
* Suggests revisions to the security program as necessary to comply with changes in the law, regulations,
professional ethics, and accreditation requirements.
Qualifications:
* Basic familiarity with the legal requirements relating to the HIPAA Security Rule, as well as the ability to
communicate with technical and non-technical personnel.
* Familiarity with all aspects of their department’s operations, especially those relating to the security of e-
PHI.
* Demonstrates organization, facilitation, communication, and presentation skills.
Data Center Security
PURPOSE
Data Center security is an important assignment of everyone working for DIO/IT. Everyone involved must accept responsibility for ensuring that staff, equipment, and facilities remain safe and available for use. A primary feature of ensuring the availability and integrity of supported information systems is to control who has physical access to the Data Center.

POLICY STATEMENT:
Sedgwick County DIO/IT shall restrict access to the Data Center to minimize risk to staff, equipment, and data.

DEFINITIONS:
1. Cleared DIO/IT employees: those individuals assigned proximity cards which allow controlled access to the Data Center by use of the card. The cards are NOT to be loaned or transferred.
2. Contractor: a company, individual, or non-DIO/IT employee contracted or assigned by the County to perform services or work within the Data Center.
3. Visitor: an individual desiring access to the Data Center who is neither a cleared DIO/IT employee nor contractor.
4. Senior Data Center employee: a DIO/IT Operator who has acknowledged responsibility for the security of the Data Center and MUST BE PHYSICALLY PRESENT IN THE DATA CENTER. This employee is responsible for checking out/in badges, knowing status of equipment and staff, and providing briefings.
5. Operators: Any DIO/IT employee whose primary job function is within the Data Center.

PROCEDURES:
Normal Data Center Access:
1. Cleared DIO/IT employees are permitted access by use of their card any time the card is valid.
2. Other County employees are visitors and are permitted access during normal working hours at the main entryway ONLY to discuss business with Data Center staff. Going beyond these areas requires signing in and a DIO/IT staff member as an escort.
3. Contractors are granted access by notifying the Data Center Supervisor of their requirement for access. In the absence of the Data Center Supervisor, contractors should contact the Tech Support Services Manager. They will notify the Data Center of expected arrivals.
   a. Contractors needing access must provide notice in advance along with this information:
      i. Who needs access (company, department)?
      ii. How many people in the work party?
      iii. What equipment or facility will they be working on and what is expected?
        (1) Dust can set off the fire suppression.
        (2) Drilling holes through walls, floors, or ceilings can reduce the effectiveness of fire suppression.
        (3) Electrical -- what’s the impact on equipment? (Motors, drills, pumps produce electrical “dirt” on power supplies.)
        (4) Outage duration and timing?
      iv. When is the contractor’s staff expected to arrive?
      v. How long will the work take?
   b. Contractors must identify themselves at a Data Center door and request entry.
   c. Contractor briefing:
      i. The Senior Data Center Person will verify the contractor’s information and require sign-in on the Data Center access log.
      ii. The contractor will provide current information concerning the work to be done.
      iii. The Senior Data Center Person will issue controlled Contractor IDs for the contractor’s staff in exchange for their Driver’s License. (One license per ID.)
      iv. The Senior Data Center Person will discuss:
        (1) safety and evacuation procedures,
        (2) keeping floor tiles in place (if appropriate)
        (3) other work that may be in process or expected,
        (4) entry/exit notification requirements,
(5) importance of physical security (blocking doors open is NOT permitted), and
(6) any other items that may be important.
d. When the Contractor’s work is completed, they will:
i. Advise the Senior Data Center Person. An inspection for cleanliness, completed work, status of equipment, and/or proper equipment operation is expected if appropriate.
ii. Check their contractor badge back in and return their Driver’s License.
iii. Sign-out of the log book.
iv. Promptly exit the Data Center.
4. Visitors are discouraged except under special circumstances. “Drop-in” visits are not permitted. When access is needed, the County employee requesting visitor access should make the request IN ADVANCE during normal business hours by notifying the Data Center Supervisor, the Technical Support Services Manager, or the CIO. During visits a DIO/IT employee will escort visitors and must stay with them, and ensure visitors sign in and out and wear visitor badges. A DIO/IT employee can escort a maximum of 3 visitors.
5. Verification. Operators are authorized to deny Data Center access to anyone who cannot provide satisfactory identification (proximity card, County ID card, or driver’s license) and justification for needing Data Center access. The visitor should be politely asked to leave, and DIO/IT management notified immediately. If necessary, Courthouse Security should be alerted.
6. Exceptions to this policy may be made by DIO/IT management by notifying the Data Center IN ADVANCE.

After Hours Data Center Access:
1. Cleared DIO/IT employees are permitted access with their card at any time the card is valid.
2. Contractors’ access procedures are the same as during normal hours.
3. Visitors are not permitted outside normal business hours unless special arrangements have been made with the Data Center Supervisor or Technical Support Services Manager.

Physical security:
1. Doors: Data Center doors will be closed and locked except when required to be temporarily open to permit staff, supplies, or equipment in/out of the data center.
2. Windows provided with blinds will have the blinds normally closed.
3. TV camera monitoring of the exits:
   a. Should be accomplished before granting access to doors.
   b. Should have recording tapes rotated to provide maximum recorded time with available tapes.

Higher Alert Status:
The Data Center may be requested to go to a higher status of alerting than normal. This will be done in person, by phone or e-mail request from Courthouse Security or DIO/IT management. Upon receiving such notice, Operators will:
1. Verify all window blinds are closed and all doors are closed and locked.
2. Require all persons not engaged in business-related activity to leave the Data Center promptly.
3. Require maintenance operations be completed and staff leave as quickly as possible.
4. Review fire suppression discharge/dump avoidance procedures. Verify location of hand fire extinguishers and floor pullers.
5. Any recent dump tapes still on-site should be sent to their normal destination immediately.

Notification to returning to normal status will be done in person, by phone or e-mail request from Courthouse Security or DIO/IT management.

Data Center Evacuation:
Because of weather, bomb or hazardous threats, or fire alarms, it may be necessary to evacuate the Data Center. NEVER PLACE JOB TASKS AHEAD OF YOUR SAFETY OR THE SAFETY OF YOUR CO-WORKERS. The following steps should be taken:
1. Make certain window blinds are closed.
2. Unless directed otherwise, leave equipment powered ON.
3. Leave ceiling lights ON.
4. Take building and room keys with you.
5. Proceed to the nearest safe location as quickly and safely as possible.
6. Notify DIO/IT management of circumstances and your location.
050 Sedgwick County, KS – Forensics Backup Procedure

FORENSICS BACKUP PROCEDURE
Document steps carefully. For copying personal information that is involved in legal cases:
1) Receipt of directive or court order (obtain actual copy):
a) Log date & time of receipt: ___/___/___ Time: ___ _____
b) Read carefully for applicability.
c) Identify the dates of information needed. Between ___/___/___ and ___/___/___.
d) Obtain Legal Department's concurrence for understanding of requirements.
e) Determine a list of individuals whose PCs may be involved.
f) Determine what to copy:
   i) C:\ Yes No
   ii) U:\ Yes No
   iii) .pst Yes No
   iv) CDs/disks Yes No
   v) Flash drives Yes No
   vi) Other: Yes No Specify: ______________________________________
2) Determine staff who will perform the work:
a) Notify applicable IT individuals that may be performing the work. Provide minimal knowledge of why
the copy is taking place.
b) Determine if anyone potentially assigned to the tasks has any conflict of interest. Do they know
anyone involved? Certification form?
c) Caution involved staff about confidentiality.
3) Obtain media for making copies of the data/information:
a) Verify the target is clean and has sufficient space for the copy.
4) Locate the PCs of the staff who were or are involved:
a) If a reassignment of the PC has occurred, use the County’s Fixed Asset number (FA#) to try to find
who has the PC now. (The County does not currently track PC reassignments.)
b) Provide four hours warning “you’ll be without your PC” to current staff concerning their copy.
5) Perform the copy as requested (may be at a copy level that gets a track-by-track image, not just a copy
of existing files). Make additional copies as required.
6) Verify logs are complete.
7) Keep all materials, notes, logs, etc in a secure environment. (Consider multiple secure locations for
backup?)
8) Log time as applicable.
I. POLICY STATEMENT

A. To provide for the information technology needs of a sophisticated government organization in an era of rapid technological advancement, the Sedgwick County Department of Information Services will provide County departments and the Eighteenth Judicial District standard options and consultation for information technology applications, including computing equipment, software, area networks, installation, systems design, programming, testing, and system implementation.

B. To assist the Department of Information Services in fulfilling its role, elected officials, bureau directors, and department heads must: protect computer equipment in their charge from physical damage or misuse; take appropriate steps to protect computer output containing sensitive information; prevent unauthorized individuals from viewing or having access to computer displays; obtain and delete user identifiers providing access to computer functions for employees and ensure that adequate internal office procedures are in place for their employees to logoff/sign-off networks when appropriate; make all reasonable efforts to assure passwords for the employees of their departments remain secure; maintain sufficient manual procedures to enable the functions of their department to continue in some limited fashion during a computer outage of any length; and assume responsibility for relocation of computer equipment.

C. Sedgwick County will comply fully with the Kansas Open Records Act (K.S.A. 45-215 et seq.) with respect to electronic data. Sedgwick County employees will not knowingly receive, install, copy, use, maintain, or provide software or any machine-readable data in violation of federal or state laws or local ordinances. Electronic and voice mail capabilities provided to employees are for official business use, and shall be subject to access by appropriate supervisory personnel without an employee’s knowledge.

II. DEFINITIONS

After-hours access – time other than when a system is normally scheduled to be available for processing.

Clients – departments and employees, and possibly members of the public or other agencies granted access to County systems by agreement.

Commercial computing networks – Internet providers, America On-Line, Prodigy, CompuServe, etc.

Computer equipment – computers or computer output devices (printers, plotters, communication devices, display terminals, personal computers).

Data record – a group of information about a particular thing or person kept together and described by a file layout.

Departmental system – a smaller computer supporting a department.

Download – the transfer of a copy of machine-readable data from an originating computer to another.

Electronic mail – computer-delivered correspondence used for communication between individuals.

Equipment – any computer, or computer output device (printer, plotter, communication devices, display terminal).

File layout – a listing of data field names, sizes, types, and relative locations within a data record.

Logoff/sign-off – a final command entered by an operator making a link to a network ineffective until another operator has correctly signed on.

On-Line Access – authorized ability to inquire upon or update information using a device connected locally or remotely to Sedgwick County computer systems.

Password – a secure combination of characters entered by a person and used by the computer to verify authorization to computer functions.

Relocation – a displacement of equipment requiring rerouting or altering the cables supporting the equipment.

Sensitive information – data, text, images, graphics, checks, or warrants that are not for general distribution or public knowledge due to legal, policy, or timing considerations.

Software – a stored sequence of machine-readable instructions that cause a machine to perform calculations or actions. Software may be purchased or created in-house.
Subscribers – private or public corporations, other governmental jurisdictions and their subdivisions, or members of the public granted on-line access on a fee basis.

Systems design – analysis of an application to determine suitability of applying automation to a process.

Upload – the transfer, by electronic means, of machine-readable data from a departmental system to another computer which has responsibility for maintaining the data.

User identifier (userid) – a non-secure combination of characters entered by an operator to uniquely identify the individual to the computer.

Voice mail – stored voice recordings used for communication between individuals, that may be manipulated (stored, forwarded, replayed, deleted) by the person for whom the recording is left.

III. PROCEDURE

A. Physical Security.
1. Departments are responsible for restricting access to equipment. This includes materials that have become “waste.”
2. Where necessary, coverings should be used to protect equipment from a hostile environment (public access, tampering, water, excessive dust or heat).

B. Information Security. Each client department’s information in a shared computer system shall be secure and unavailable to other clients without permission. The intent is not to discourage AUTHORIZED access or use of information managed in support of another client. Elected officials, bureau directors, and department heads must have legal authority (refer to K.S.A. 45-221) to deny access to other departments or members of the public.
   1. On-line access to client information is normally controlled by the responsible department. Requests for access should be made to the appropriate department.
   2. For other access to client information, authorization from the controlling department should be requested in writing. The controlling department should respond in writing to the requestor with a specific grant or denial of access.

C. Computer Access and Passwords.
1. Each department will have a departmental security administrator, who is the elected official, bureau chief, or department head responsible for that department, or an individual designated by that person. Such designation shall be made in writing to the Director of Information Services. Departmental security administrators are authorized to obtain, change, or delete user identifiers, and authorize access to functions on menu(s) managed by the department.
2. Each individual needing access to the computer should be assigned a unique user identifier. In the event that an individual’s user identifier expires or is suspended, it shall be the responsibility of that individual to inform their departmental security administrator.

1. Disaster recovery procedures should be considered an integral part of the requirements when a system is being designed or purchased.
2. Elected officials, bureau directors, and department heads should periodically review their procedures to verify the validity of the backup.
3. Information Services shall provide consulting help concerning the adequacy of backup procedures.

E. On-Line System Availability. Information Services provides on-line access according to schedules. Where possible, requests for after-hours access will be accommodated. Requests for additional support time should be:
   1. Made AT LEAST 24 hours in advance.
   2. Directed to the department’s assigned IS Project Leader who shall coordinate the effort to determine if schedules may be adjusted to accommodate the request. Normally, if an on-line system is available to support a client, they system is also available to any other client using that system.

F. Copyrighted Materials. To protect against the possibility of copyright infringement, departments must maintain a list of all software products installed on computing equipment under their control. The purchase order number and date should be supplied for each product.

G. Central Server Downloads to Personal Computers and Departmental Systems. All security measures that apply to obtaining access to information apply to downloading data to a departmental system.
   1. Client departments desiring to download data will:
      a. Determine if the data desired are available and obtain proper authorization to access the data from another client if necessary.
b. Contact Information Services to discuss availability of data, frequency of the download, desired formatting, and proper authorization.
c. Work with Information Services to accomplish the file transfer.

2. Information Services will:
   a. Verify proper authorization and provide the data desired by the client.
   b. If the transfer is to be done on a regular basis, the job(s) will be set up as a production job(s).

1. Uploading of data will be permitted under the following circumstances:
   a. The data is entered in an approved method to provide maximum editing and validation checks prior to the upload and is formatted so that it will be compatible with existing programs.
   b. Storage capability is available for maintaining and/or backing up the data in machine-readable form and off-loading smaller systems.

2. Client departments desiring to upload data should contact their assigned IS Project Leader to discuss availability of space, frequency of the upload, formatting required, and validation necessary.

3. Information Services will:
   a. Provide data formats and describe edit checking that may be done to validate data prior to upload.
   b. Monitor the transfer of data from the departmental system.
   c. If the transfer is to be done on a regular basis, the job will be set up and put into production.

I. Subscriber Access to Information.
1. On-line access to data files of the Appraiser’s Office, County Clerk, County Court, Eighteenth Judicial District Court, Election Commissioner, Register of Deeds, and Treasurer residing on Sedgwick County computer systems may be available to subscribers.

2. Requests for subscription shall be made to Information Services. The potential subscriber will be required to properly execute a standard service contract. Any deviations to the standard service contract must be approved by the Legal Department. All contracts require Board of County Commissioners approval.

3. Information Services may provide demonstrations using County equipment at a potential subscriber’s site for a period not to exceed sixty (60) days.

4. Subscribers with access to computer applications may be granted access to additional functions by requesting access from the elected official, bureau director, or department head responsible for maintaining the information.

J. Compliance With Open Records Requests.
1. Requestors asking for copies of information should be provided a copy of this procedure.

2. Requests must be made in writing, specifying what data are desired. It is helpful to be as explicit as possible; copies of existing reports or screens with the desired information marked on them are particularly helpful.

3. The appropriate custodian/responsible department will analyze the request and provide a written cost estimate for the request:
   a. Staff time.
   b. Computer time – at current rate.
   c. Output media – normally paper. If an electronic (machine readable) copy is desired, it will be provided on the highest density media of devices attached to the computer processing the information to minimize labor. If applicable, tapes will carry manufacturer’s standard (internal) labels.
   d. Where possible, standard utilities will be used to copy requested files.
   e. Programming will be limited to removing information restricted by law (K.S.A. 45-221(d)).
   f. If the contents of a field refer to a table of information, a copy of the table will also be provided.
   g. File layouts will be provided for all machine-readable files.

4. Requestors shall provide a signed acknowledgment of the estimate and a check for that amount (K.S.A. 45-218(f)). Any excess fee will be refunded; the requestor remains responsible for any amount over the estimate.

5. The requestor shall acknowledge they have a responsibility to use the information in compliance with Kansas law (K.S.A. 21-3914 and 45-220(c)).

1. Employees with access to commercial computing networks provided by the County shall:
   a. Restrict activity to legitimate County business.
b. Not attempt to express personal opinions as representative of the County.

2. Elected officials, bureau directors, and department heads will verify that requests for access to commercial computing networks are for valid business purposes.
Acceptable Use Agreement
For Information Technology
I understand that by using information technology on Sedgwick County equipment or time, this technology
is provided by Sedgwick County at the County's expense, and therefore is the County's property. I
understand this information technology is provided for use for County business transactions, research,
records, and communications. I understand that no one is to receive access to information technology
without signing this agreement, and that violation of this provision may subject me to discipline up to and
including termination. Information technology includes Internet access, electronic mail and voice message
systems, facsimile devices, or other electronic systems used by Sedgwick County.
I understand and agree that:
• Electronic mail is an extension of Sedgwick County Government.
• Electronic mail messages can be traced to the sender and recipient even after deleted from computers.
• The County may be legally required to produce evidence of my use of information technology for
matters of litigation, pursuant to the Kansas Open Records Act, and other purposes.
• I will not knowingly communicate, download, or forward anything that might be construed as harassing,
hostile, or offensive to others based on ethnicity, race, sex, disability, age, religion, or national origin.
• I will not use the County’s information technology to solicit non-County business for any personal cause,
including political or religious issues.
• I will not send to multiple recipients electronic mail with non-County business content.
• I will not knowingly display, print, download, or send any questionable image or message.
• I will immediately advise anyone sending me improper or questionable material that such transmissions
should stop.
• I will not open items that the virus scanner has warned contains a virus and will delete such items
immediately.
• I will abide by the County’s Information Technology Usage policy and procedures.
• I will not use County information technology for inappropriate uses. If I have a question about whether a
use is inappropriate, I will contact my supervisor.
Examples of inappropriate uses of information technology include, but are not limited to:
-- Illegal activities
-- Gaming: betting, gambling, wagering
-- Representing personal opinion as that of the County
-- Unauthorized solicitations
-- Revealing unauthorized or confidential information
-- Slander, libel, deliberate misinformation
-- Accessing pornographic material for other than law-enforcement purposes
I understand that I have no expectation of privacy in my electronic communications, use of County
property, or Internet access. Sedgwick County reserves the right to review, audit, or monitor any County
information technology that I use.
Information Technology Usage
SUBJECT: Sedgwick County Information Technology Usage Policy
I. PURPOSE
Sedgwick County encourages all employees using information technology to become adept in its use.
Information technology includes Internet access, electronic and voice message systems, facsimile
devices, or other electronic systems used by Sedgwick County. It is the County’s goal to:
• Improve efficiency and effectiveness
• Develop e-workers better able to provide e-government services
• Improve productivity allowing a shift from labor-intensive tasks to higher-value results
• Improve service delivery to customers and citizens
Scope. This policy applies to all divisions, departments, contracted entities, and other individuals or
groups that use County equipment. Any of these arms of Sedgwick County Government may develop
more specific information technology policies for application within the department or division, but none
may write more lenient policies.
II. POLICY STATEMENT
Subject Matter. The subject matter of messages should demonstrate good judgment and reflect the
professionalism of Sedgwick County. Content should pass the test of being able to appear in the
newspaper without being embarrassing or offensive to anyone. Avoid whatever could be construed as
improper or embarrassing to the County. Specifically prohibited are political activity and campaigning,
religious messages or slogans, illegal activity, and use for a personal business enterprise. Use care not
to divulge confidential or sensitive information.
County Business. Information technology should be used only for official County business. Care should
be taken to limit the number of persons outside the organization who know your County e-mail address.
By doing this, you will limit the number of unsolicited, personal, and offensive messages received. Server
space is limited and should be reserved for County use. Announcements intended for all County
employees shall be sent to the Communications Office
for approval, editing, and sending.
Personal Use. Brief and occasional messages of a personal nature may be sent and received. Sending
chain letters is prohibited. Personal messages shall not impede County business. Great care and self-
control should be exercised by employees not to send multiple recipients messages with non-County
business content – for example, jokes, anecdotes, or gossip. Mass mailings and large attachments
overload the County server thereby hindering legitimate County communications. Only incidental amounts of employee time (time periods comparable to reasonable breaks during the day or during meal periods) may be used to attend to personal messages. Employees should, upon receiving a personal message, read or listen to the message and delete it in a timely manner.
County printers and paper are not for personal use.
Unknown Sources. Take extra caution when receiving a message from an unknown source, especially
from an address exterior to the County’s e-mail system. The potential to spread viruses is significant, and
opening such a message could have devastating results to the entire County system. This also applies to
attachments. “When in doubt, throw it out.”
Network Security. Everyone has an obligation to protect County computer systems and information by
adhering to good security practices that limit the threat of unauthorized use, disclosure, modification,
destruction or abuse. The Division of Information & Operations (DIO) will provide a system of user
identification (user-ids), passwords, and other network security standards.
Everyone is responsible for activity performed with their personal user-ids and is prohibited from
performing unauthorized activity with other user-ids. All internal and external connections to the Sedgwick
County Network shall be approved by DIO. Inbound dial-up access will be given only in cases of bona
fide need and when no other more secure method is available. No one shall attempt to gain access to
systems without proper authorization or use hardware or software tools on the Network that could be
used to evaluate or compromise security.
All software and files obtained from non-Sedgwick County sources via the Internet or any other network must be screened with virus-detection software prior to being used. Use caution in downloading software. Adhere to copyright laws and be aware that screen savers, backgrounds, and other such files often contain viruses that will infect computers and networks. File downloads should only occur for County business purposes. All suspected information security incidents must be reported to the Customer Support Center (helpdesk) upon discovery.

III. PROCEDURES
Audits. Law enforcement officials may examine any relevant electronic transactions in the course of an ongoing investigation of criminal activity.
Unauthorized viewing or retrieval of another person’s electronic or voice mail and other forms of electronic snooping are prohibited. The County will not routinely monitor the contents of electronic or voice mail.
Privacy. No one should expect a right to privacy in the use of County equipment. Without his/her knowledge, access to an individual’s (1) electronic or voice messages, (2) addresses accessed on the Internet, or (3) data on County equipment that has been used by an employee may be obtained by the responsible elected/appointed official or division director, or designee, for needs arising in the normal course of business. No staff or contractors of the Division of Information & Operations (DIO) shall provide access to such information unless specifically authorized by the Chief Information Officer, or designee.
Enforcement. The management of each organization using Sedgwick County information technology is responsible for communicating and enforcing this policy. No one shall receive access to the Internet or electronic or voice mail until he/she has agreed in writing to comply with this policy. Such documentation shall be retained in the respective departments. The Division of Information & Operations shall administer and enforce this policy and shall provide any procedures or forms when needed.
Sedgwick County Information Technology Usage Policy
Procedures for Enforcement

No employee should expect a right to privacy in the use of County equipment. With or without his/her knowledge, access to an individual’s (1) electronic or voice messages, (2) addresses accessed on the Internet, or (3) other data on County equipment that has been used by an employee may be obtained by the responsible elected/appointed official or division director, or designee, for needs arising in the normal course of business.

Elected/appointed officials, division directors, department heads, or the Human Resources Director, who through personal observation or by complaint suspect inappropriate uses of information technology, may utilize the following process for audit and enforcement of this policy. Inappropriate uses of information technology include, but are not limited to:
- Illegal activities
- Gaming: betting, gambling, wagering
- Representing personal opinion as that of the County
- Unauthorized solicitations
- Revealing unauthorized or confidential information
- Slander, libel, deliberate misinformation
- Accessing pornographic material for other than law-enforcement purposes.

1) Department Head obtains the departmental file copy of the employee’s signed Acceptable Use Agreement.
2) Department Head, in a time and manner that will not attract suspicion of other employees, shall request that the employee in question to log on and allow the Department Head to check the employee’s computer or other information technology equipment for suspected inappropriate usage. This may include temporary internet files or deleted and sent e-mail files, etc. Employee should be present during this review.
3) If probable violations of the IT Usage Policy are found, Department Head immediately contacts DIO Chief Information Officer to temporarily deactivate the employee’s userid and request to capture and preserve the employee’s computer or other information technology history for the suspected time frame for use in further investigation.
4) Department Head contacts at least one member of the Information Technology Usage Committee for further action, including review of captured and preserved computer history. Committee members include: The Assistant County Manager for DIO (Charlene Stevens), 660-9393, the Human Resources Director (Jo Templin), 660-7057, or Asst. County Counselor (Jennifer Magana), 660-9340. If two or more members of this committee authorize further investigation, proceed to Step 5. If there are not two or more members authorizing further action, Charlene Stevens will so notify the Department Head. When contacting the Committee, the Department Head should be as specific as possible with regard to the suspected inappropriate usage, including, date, time, etc. Department Head should also understand that if requests to DIO are not made in a timely manner, it may not be possible to recover relevant information.
5) The Assistant County Manager reviews content of preserved history of suspected inappropriate uses of information technology, and reviews findings with Department Head and Committee. The Sheriff Department is immediately contacted in cases of suspected criminal activity.
6) The Information and Technology Committee and Department Head will determine further action.
Sedgwick County Non-Employee Information Technology Usage Agreement

1. Non-employee personnel have no expectation of privacy in any electronic communications, use of Sedgwick County property, or Internet access. Sedgwick County reserves the right to review, audit, or monitor any information technology used by non-employee personnel.

2. Non-employee personnel shall use only accounts authorized by the Sedgwick County Chief Technology Officer (SCCTO).

3. Non-employee personnel may access only those resources for which they are specifically authorized.

4. Non-employee personnel are personally responsible for safeguarding their account and log-on information. Passwords shall adhere to the following:
   a. Passwords shall remain confidential.
   b. Passwords shall be changed at least every 90 days.
   c. Passwords shall be at least six characters long.
   d. Passwords shall contain characters from at least three of the following four classes:
      (i) English upper case letters, A, B, 
      (ii) English lower case letters, a, b, 
      (iii) Westernized Arabic numerals, 0, 1, 2, and 
      (iv) Non-alphanumeric ("special characters") such as punctuation symbols.
   e. Passwords shall not contain your user name or any part of your full name.
   f. Passwords shall never be displayed, printed, or otherwise recorded in an unsecured manner.

5. Non-employee personnel are not permitted to script their user IDs and/or passwords for log-on access.

6. Non-employee personnel are not permitted to allow another person to log-on to any computer utilizing their, if provided, personal account, nor are they permitted to utilize someone else's account to log-on to a computer. Authorized system or service accounts may be used by multiple authorized people.

7. Non-employee personnel may not leave their workstation logged onto the network while away from their area. Non-employee personnel may elect to lock the workstation rather than logging off when leaving for very short time periods.

8. Non-employee personnel shall maintain a log, left with the computer, of all software loaded onto any Sedgwick County computer. The software must have been approved in writing in advance by the SCCTO.

9. Non-employee personnel shall execute only applications that pertain to their specific contract work.

10. Non-employee personnel shall promptly report log-on problems or any other computer errors to the Helpdesk (316-660-9811).

11. Non-employee personnel shall promptly notify the SCCTO if they have any reason to suspect a breach of security or potential breach of security.

12. Non-employee personnel shall promptly report anything that they deem to be a security loophole or weakness in the computer network to the SCCTO.

13. Non-employee personnel shall not install or use any type of encryption device or software on any Sedgwick County hardware, which has not been approved in writing in advance by the SCCTO.

14. Non-employee personnel shall not attach any device to the Sedgwick County network without prior written approval in advance from the SCCTO.

15. Non-employee personnel may not remove any computer hardware, data or software from a Sedgwick County building for any reason, without prior written approval from the SCCTO.

16. Non-employee personnel shall not delete, disable, or bypass any authorized encryption device, or anti-virus or other software program, installed on Sedgwick County hardware.

17. Non-employee personnel shall not attach any network or phone cables to any Sedgwick County device without written approval from the SCCTO.

18. Non-employee personnel may not copy any data and/or software from any Sedgwick County resource for personal use.

19. Non-employee personnel may not utilize Sedgwick County computer systems or networks for any of the following reasons:
   a. Game playing;
   b. Internet surfing not required for their work activity;
   c. Non-related work activity; or
d. Any illegal activity.
e. Downloading of files from non-County resources. If files are needed for your work, contact Sedgwick County DIO IT personnel.

20. Non-employee personnel are prohibited from intercepting or monitoring network traffic by any means, including the use of network sniffers, unless authorized in writing in advance by the SCCTO.

21. Non-employee personnel may not give out any Sedgwick County computer information to anyone. Exception: other non-employee personnel needing the information to complete authorized tasks and who have signed this agreement. Information includes but is not limited to: IP addresses, security configurations, etc.

22. All data storage media shall be erased or destroyed prior to disposal.

23. Non-employee personnel may not remove, modify, erase, destroy or delete any computer software without the written approval in advance of the SCCTO.

24. Non-employee personnel shall not attempt to obtain or distribute Sedgwick County system or user passwords.

25. Non-employee personnel shall not attempt to obtain or distribute door passcodes/passkeys to secured rooms at any Sedgwick County facility for which they are not authorized.

26. All equipment issued to non-employee personnel will be returned in good condition to Sedgwick County upon termination of the Sedgwick County/non-employee Personnel relationship.

27. Non-employee personnel may not use Sedgwick County information technology to send or receive threatening, obscene, abusive, sexually explicit language or pictures.

28. Non-employee personnel are prohibited from causing Sedgwick County to break copyright laws.

29. Use by non-employee personnel of any Sedgwick County information technology will acknowledge acceptance of the above referenced policies. Any non-employee who violates any of these policies shall be subject to disciplinary action, including total removal from the Sedgwick County project as well as being subject to Kansas civil and criminal liability. Disciplinary action may include Sedgwick County requesting the non-employee be considered for demotion, suspension and termination.

Anyone that is not a Sedgwick County employee who will access Sedgwick County information technology in the course of their work for Sedgwick County (“Non-employee personnel”) are required to sign this document before accessing any Sedgwick County information technology system. “Information technology” includes any computer, network, Internet access, electronic mail and voice message systems, facsimile devices, or other electronic systems used by Sedgwick County.
PCI SECURITY STANDARDS
What kind of a scan needs to be performed?
Vulnerability Assessment Scans must be performed by Payment Card Industry Approved Scanning Vendors (ASV). The scan will be performed over all externally facing IP addresses that touch the credit card acceptance, transmission and storage process. Scans must be turned into the merchant bank on a quarterly basis.
There are six categories of PCI compliance security standards.
1. Build and Maintain a Secure Network
   a. Requirement 1: Install and maintain a firewall configuration to protect cardholder data
   b. Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data
   a. Requirement 3: Protect stored cardholder data
   b. Requirement 4: Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program
   a. Requirement 5: Use and regularly update anti-virus software
   b. Requirement 6: Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures
   a. Requirement 7: Restrict access to cardholder data by business need-to-know
   b. Requirement 8: Assign a unique ID to each person with computer access
   c. Requirement 9: Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks
   a. Requirement 10: Track and monitor all access to network resources and cardholder data
   b. Requirement 11: Regularly test security systems and processes
6. Maintain an Information Security Policy
   a. Requirement 12: Maintain a policy that addresses information security
Additional Information:
1. Payment Card Industry (PCI) Data Security Standard -- Self-Assessment Questionnaire
   https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf
   https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf
Records Management POLICY

III. All County records belong to the citizens of Sedgwick County. County divisions / departments are the custodians of records they create or receive in doing the public's business. County records are information assets, and must be accessible to the full extent allowed by law to all citizens for the conduct of public and private business, and for citizens to use in monitoring the performance of their County government. (KSA 45-403(a))

The Kansas Government Records Preservation Act charges counties with the responsibility to preserve "records with enduring value," to properly arrange records "so that appropriate public access is possible," and to dispose of "noncurrent records which do not merit preservation [which] will promote economy and efficiency in the day-to-day activities of government." (KSA 45-401)

PURPOSE OF THE RECORDS MANAGEMENT PROGRAM

The purpose of the Records Management program is to assist divisions / departments in effectively and efficiently managing County records throughout their life cycle, from creation to ultimate destruction or archival retention, and to meet the diverse needs of citizens, policy makers, management and administrative users for access, preservation and disposal.

FUNCTIONS OF THE RECORDS MANAGEMENT PROGRAM

Records Management (RM) will have the following set of interrelated functions:

Legal responsibility — Develop and implement policy, procedures and programs to meet the County's responsibility under State law to retain, preserve and dispose of public records in a systematic, business-like manner.

Retain & dispose — By means of policy, procedures, inventories, retention schedules and training, retain records as long as they represent administrative, legal, fiscal or enduring archival value, and promptly dispose those records that no longer have value.

Public access — Enhance citizens' access to public records, with particular attention to preserving those records that document Sedgwick County's historical heritage.

Cost effectiveness — Make record keeping more efficient, less costly and more responsive and effective as a tool for providing quality services to citizens by means of policy, implementing procedures, training for employees, assistance to and partnering with departments, and cooperation with State and community agencies.

Vital records — Safeguard the County's vital records, those that are essential to maintain rights and essential legal and fiscal interests, for both the County and its citizens.

Records as a resource — Make the County’s public records more accessible, more useful and more frequently used as a resource to support policy making, diverse research and informed discussion of public issues.

DEFINITIONS

A record is recorded information, regardless of medium or characteristics, made or received by an organization, that is useful in the operation of the organization.

A records series is a group of similar or related records that are normally used and filed as a unit and can be evaluated as a unit for determining the records retention period.

The retention period for a records series is the time the records must be kept to satisfy legal and/or organizational requirements.

"Government Records' means all volumes, documents, reports, maps, drawings, charts, indexes, plans, memoranda, sound recordings, microfilms, photographic records and other data, information and documentary material, regardless of physical form or characteristics, storage media or condition of use, made or received … in … transaction of official business." (KSA 45-402(d))

Non-records for purposes of Kansas records law include (but are not limited to) "[p]ublished material acquired and preserved solely for reference purposes, extra copies of documents preserved only for convenience of reference and stocks of publications, blank forms and duplicated documents …" (KSA 45-402(d))
Disposition is the final action for records, normally occurring at the end of their retention period. Records may be disposed by either destruction or by archiving, which means conveying them to an internal archival function or eligible, external archival agency.

A records center is a centralized, lower cost area for housing and servicing inactive or semi-active records whose reference rate does not warrant their retention in the prime office area.

Records Management is the systematic control of all records from their creation, or receipt, through their processing, distribution, organization, storage and retrieval to their ultimate disposition.

ADMINISTRATIVE RESPONSIBILITIES & PROGRAM MANAGEMENT
The Records Manager will be responsible for overall planning, development and administration of the Records Management Program. The Program will be organizationally located in the Division of Operations, or elsewhere as directed by the County Manager, as a central function to serve all divisions / departments.

Liaison with State – The Records Manager will serve as liaison with the Kansas State Historical Society (KSHS), the agency tasked by the Kansas Legislature to implement the Kansas Government Records Preservation Act. (KSA 45-401 et seq.)

Establish standards, procedures and guidelines – The Records Manager will establish such standards, procedures and guidelines as are necessary to implement this policy.

Advise departments in applying technology – The Records Manager will advise departments in projects that apply technology to managing records, to ensure that systems will meet County access needs throughout the full retention period and meet legal requirements. The Records Manager will assist Budget staff in reviewing requests to acquire film / digital imaging systems and services, consistent with County Resolution 193-1996.

Training – The Records Manager will train Records Coordinators and other County employees who create, use and manage records in this policy, in any related policies, implementing procedures, standards and guidelines, and in records management methods and practices.

A Records Management Advisory Committee will represent a cross section of customer divisions / departments and both internal and external stakeholders, in planning and developing the RM program, setting goals and objectives, and otherwise assisting the Records Manager in implementing the program. Included within membership of the Committee will be representatives of the County Counselor’s Office and Finance.

Records Coordinators – Each elected County official, division director and department director responsible for making and keeping records will appoint a records coordinator, who will assist the Records Manager in achieving the RM program’s objectives. Each Records Coordinator will be primarily responsible for conducting records surveys, inventories and other records management tasks at the divisional / departmental level, with the assistance of the Records Manager.

RETENTION OF RECORDS
The Records Manager will determine retention periods for records series, consistent with State retention schedules and in consultation with custodial divisions / departments, the County Counselor’s Office and any other divisions / department(s) affected.

Until such time as the County adopts its own retention schedules and obtains approval from the State Records Board, the Records Manager will apply State “retention and disposition schedules” (KSA 45-404(g)) promulgated by the KSHS to implement the Government Records Preservation Act (KSA 45-406(d)), which are mandatory for counties (KSA 45-404(b)).

The Records Manager will consult with the State (KSHS) to clarify definitions of records series and retention periods, as necessary.

In any case in which a retention period requirement for a records series is found to be excessively long or otherwise inconsistent with County needs, any petition for exception to the State Records Board first shall be submitted by the Records Manager to the County Manager and the Board of County Commissioners for approval.

In any case in which the County cannot find a records series retention listed in the State “retention and disposition schedules,” any request to the State Records Board for authority to dispose first shall be submitted by the Records Manager to the County Manager and the Board of County Commissioners for approval.

STORAGE OF INACTIVE RECORDS
Inactive records series, those accessed once per month or less often on the average, should be stored outside of administrative offices, at lower-cost commercial, divisional / departmental or shared County
records storage facilities, whenever economical. All off-site storage facilities must provide adequate physical security and meet appropriate environmental standards for the media involved.

The Records Manager will establish standards and procedures for the storage of inactive records, including boxes, labeling, storage logs and records management software. Records storage facilities will store records and RM-related materials exclusively. They will not be used to store office supplies, surplus equipment or other materials not related to the management of County records.

All costs for storage of and access to inactive records at off-site commercial storage sites will be borne by custodial divisions / departments. The Records Manager will monitor the use by divisions / departments of off-site commercial storage for inactive records and the costs of access services. The Records Manager will ensure that all commercial storage sites provide appropriate environmental and security conditions for the records stored.

The Records Manager will plan, develop and manage any County records center(s) which may be implemented to store inactive records and to provide other RM services. Inactive records stored in a commercial site or at a County records center will remain in the legal custody of the originating division / department, until such time as they may be formally conveyed to RM for archival retention or other disposition.

The custodial division / department will be responsible for authorizing access to inactive records stored at commercial sites or at County records centers. RM will refer all requests, whether from other County divisions / departments or from the public, for access to records to custodial divisions / departments.

When a division / department conveys records to RM for archival retention, it transfers all rights and responsibilities associated with those records, including granting access, decisions as to preservation and costs of retention. Similarly, rights and responsibilities would transfer with any records conveyed to a non-County archival agency.

**DISPOSITION OF RECORDS**

To minimize costs to the public and to reduce the potential for legal liability, it will be standard County practice to proceed to dispose of records as soon as they have reached the minimum retention period set in applicable retention schedules. Each division / department will create a procedure for periodic disposal of records that integrates with its other administrative processes.

The Records Manager will advise and assist divisions / departments in developing records disposal procedures and in all disposals of eligible records.

Divisions / departments will submit all requests to dispose records to the Records Manager, who will analyze; obtain reviews of legal, fiscal and archival values, and present findings and recommendations to the Board of County Commissioners for action.

No record that is potential evidence in litigation, administrative or regulatory proceedings or that is needed for performance of a prospective financial audit will be disposed, even if the established retention period has been satisfied.

Certain internal electronic mail and Internet electronic mail may be “government records” and should be printed by the originator or recipient (for those received external to the County organization) and filed with paper files of correspondence, case files, project files or other appropriate records series, or included within a digital records keeping system. The originator of electronic mail messages (or the recipient, for email received from external sources) will have the primary responsibility to determine whether the electronic communication documents a transaction of official County business that is otherwise undocumented.

Disposition of records may be by destruction, by conveying to an archival institution as provided by law (KSA 45-404(d)), or by transfer to the control of RM for archival retention.

The standard means of destruction for records will be by commercial recycling, documented by a “certificate of destruction” obtained from the vendor. Records containing confidential information may be shredded prior to recycling, if recommended by the Records Manager and approved by the Board of County Commissioners.

All disposals of County records require approval by the Board of County Commissioners of a resolution ordering their disposal. (KSA 45-404(c)) An inventory of records disposed and a cost analysis of the disposal (when commercial storage cost data is available) will be provided by the Records Manager in support of the recommended action.
An order by the Board of County Commissioners to dispose a records series by destruction will require destruction of all duplicate and use copies of the records series, in whole or in part, held by any County division / department or employee.

Costs of records disposals will be borne by the custodial department, unless another source of funds is proposed to and approved by the Board of County Commissioners.

The Records Manager will maintain a permanent record of all records disposed.

**DISPOSITION OF “NON-RECORDS”**

Only the “copy of record” should be retained for the full retention period. Duplicate, “use” or convenience copies of a record should be destroyed as soon as their current administrative purpose has been served, which in all cases should be less than that of the copy of record. No duplicate copies of any record shall be retained, in any form by any department and by any employee, past the destruction of the records series approved by the Board of County Commissioners.

The Records Manager will assist departments in determining whether documents are duplicates, subsets of “copies of record,” interim drafts which have been superceded, or are otherwise “non-records,” which may be disposed without application of the formal disposal process, and which are “government records,” which require approval by the Board of County Commissioners to dispose.

Non-record duplicates containing confidential information should be definitively destroyed in the same manner as the copy of record, and such destruction should be documented and retained at the division / departmental level.

Informal notes, drafts and other routine working papers of employees are non-records and should be disposed as soon as their current administrative purpose has been served.

An employee’s personal and private materials neither made nor received in connection with the transaction of County business are non-records, even if physically located at an employee’s workstation on County premises.

To the extent possible, internal electronic mail communications should be used as the functional equivalent of informal telephone or in-person conversations, which do not document transactions, decisions or findings and are not “government records.” Internal electronic mail communications may be used to confirm or reinforce internal memoranda and other records. Users should delete non-record internal electronic mail messages as soon as they no longer have value in accomplishing their current work.

Voice mail messages should be used as the functional equivalent of informal telephone or in-person conversations, which do not document transactions, decisions or findings and are not “government records.” However, voice mail may be used to confirm or reinforce internal memoranda and other records. Users should delete voice mail messages as soon as they no longer have value in accomplishing their current work. The County’s voice mail system is not designed as a system for making and retaining records: it automatically deletes messages after short periods, deleted messages cannot be restored, and messages are not included in system backups.

Internet electronic mail communications (e-mail) that replace written / faxed correspondence, document purchases, or otherwise record transactions should be printed and filed with the appropriate functional records series. Those e-mail messages that represent the functional equivalent of informal telephone or in-person conversations and which do not document transactions, decisions or findings are not “government records.” Users should delete “non-record” e-mail messages as soon as they no longer have value in accomplishing their current work.
Software Compliance and Usage

OFFICE WITH PRIMARY RESPONSIBILITY:
Division of Information & Operations

I. PURPOSE
The intent of this policy is to bring all elements of Sedgwick County government into compliance with current and all future licensing agreements addressing the use of software / programs that Sedgwick County enters into, greatly reducing the possible financial liability on the part of Sedgwick County. It must be remembered that none of the software programs loaded on Sedgwick County’s systems are owned by the county, unless written by one of our programmers, they are only leased, in many cases these leases are for a very specific time period.

Scope. This policy applies to all divisions, departments, contracted entities, and other individuals or groups that use County equipment.

II. POLICY STATEMENT
It is the policy of Sedgwick County to respect all computer program / software copyrights and to adhere to the terms of all program/software licenses to which Sedgwick County is a party. Sedgwick County will take all steps necessary to prohibit users from duplicating any licensed programs/software or related documentation for use either on Sedgwick County premised or else where unless Sedgwick County is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of program / software may subject users and / or Sedgwick County to both civil and criminal penalties under the United States Copyright Act.

Sedgwick County will not permit any employee to use program / software in any manner inconsistent with the license agreements, including giving or receiving program / software or fonts from clients, contractors, customers and others.

III. DEFINITIONS
A computer program, under the Copyright Act, is defined as “a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.” 17 U.S.C. 101

A copy, as that term is used in the Copyright Act, is any material object, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. 17 U.S.C. 101

A copyright is the exclusive right granted to authors under the U.S. Copyright Act to copy, adapt, distribute, rent, publicly perform, and publicly display their works of authorship, such as literary works, databases, musical works, sound recordings, photograph and other still images, and motion pictures and audiovisual works.

A copyright owner, with respect to any one of the exclusive rights comprised in a copyright, refers to the owner of that particular right. 17 U.S.C. 101

A license is a contract in which a party with proper authority grants permission for another party to do something that would otherwise be prohibited.

Software / program piracy is the unauthorized use of software. Types of piracy include: 1) purchasing a single user license and loading it onto multiple computers or a server (softloading); 2) making, distributing and / or selling copies that appear to be from an authorized source (counterfeiting); 3) renting software without permission from the copyright holder; 4) distributing and / or selling software that has been “unbundled,” or separated, from the products with which it was intended to have been “bundled”; and 5) downloading copyrighted software from the Internet or bulletin boards without permission from the copyright holder.

Publication, under the Copyright Act, is the distribution of copies of a copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies to a group of persons for purposes of further distribution, public performance, or public display also constitutes publication. A public performance or display of a work does not of itself constitute publication. 17 U.S.C. 101

The term reproduction right refers to the exclusive right granted to the owner of a copyright to make (and authorize others to make) copies of his or her work. 17 U.S.C.106
The copyright holders for shareware allow purchasers to make and distribute copies of the software, but demand that if, after testing the software, you adopt it for use, you pay for it.

Some laws provide a threshold level of damages, called statutory damages. One such statute is the Copyright Act, which provides that the plaintiff may recover between $500 and $100,000 for each copyright work infringed by the defendant, regardless of whether he or she was able to prove in court that he or she has actually been damaged. 17 U.S.C.504

IV. PROCEDURES

Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by software manager or designated department, is a violation of copyright law.

User Education. Sedgwick County will provide and require a software education program for all of its software users (to be crafted by the Software License & Records Analyst). Upon completion of the education program, users are required to sign Sedgwick County’s Employee Personal Computer Software Usages Guidelines. New users will be provided the same education program within 30 days of the commencement of their employment.

Budgeting for Software. When acquiring computer hardware, software and training, Sedgwick County must budget accordingly to meet the costs at the time of acquisition. When purchasing software for existing computers Sedgwick County must charge the purchases to the department’s budget for information technology or an appropriate budget set aside for tracking software purchases.

Acquisition of Software. All software acquired by Sedgwick County must be purchased through Purchasing Department. Software may not be purchased through user corporate credit cards, petty cash, and travel or entertainment budgets. Software acquisition channels are restricted to ensure that Sedgwick County has a complete record of all software that has been purchased for Sedgwick County computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Registration of Software. When Sedgwick County receives the software, the Software License & Records Analyst must first receive the software first to complete registration and inventory requirements before installation. In the event the software is shrink-wrapped, Software License & Records Analyst is responsible for completing the registration card and returning it to the software publisher. Software must be registered in the name of Sedgwick County and department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user. The Software License & Records Analyst will maintain a register of all Sedgwick County’s software and will keep a library of software license. The register must contain: a) the title and publisher of the software; b) the date and source of software acquisition; c) the location of each installation as well as the serial number of the hardware on which each copy of the software is installed; d) the existence and location of back-up copies; and e) the software product’s serial number.

Installation of Software. After the registration requirements above have been met, the software will be installed by DIO – Customer Support. Once installed, the original media will be kept in a safe storage area maintained by the Software License & Records Analyst, in the Courthouse Records Center. User manuals, if provided, will be either reside with the user or reside with Software License & Records Analyst, in the Courthouse Records Center.

Home Computers. Sedgwick County’s computers are organization-owned assets and must be kept both software legal and virus free. Only software purchased through the procedures outlined above may be used on Sedgwick County’s machines. Users are not permitted to bring software from home and load it onto Sedgwick County’s computers. Generally, organization-owned software cannot be taken home and loaded on a user’s home computer if it also resided on a Sedgwick County’s computer. If a user is to use software at home, Sedgwick County will purchase a separate package and record it as an organization-owned asset in the software register. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. If a user needs to use software at home, he/she should consult with the Software License & Records Analyst or designated department to determine if appropriate licenses permit home use.

Shareware. Shareware software is copyrighted software that is distributed via the Internet. It is the policy of Sedgwick County to pay shareware authors the fee they specify for use of their product. It must be remembered that most shareware is free for personal use, downloading onto Sedgwick County equipment is not considered personal use and requires Sedgwick County to pay for a license. Under this
policy, acquisition and registration of shareware products will be handled the same way as for commercial software products.

Periodical Audits. The Software License & Records Analyst or designated department will conduct periodical audits of all Sedgwick County’s PC’s and servers, including portables, to ensure that Sedgwick County is in compliance with all software licenses. Surprise audits may be conducted as well. Audits will be conducted with using an auditing software product. Also, during the periodical audit, Sedgwick County will search computer viruses and unauthorized downloads and eliminate any that are found. The full cooperation of all users is required during audits.

Penalties and Reprimands. According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as $150,000 per title infringed, and criminal penalties, including fines as much as $250,000 per title infringed and imprisonment of up to five years. A Sedgwick County user who make, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. Such discipline may include termination of employment. Sedgwick County does not condone the illegal duplication of software and will not tolerate it.

Sedgwick County Employee Usage Guidelines For Software Usage

Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by Software License & Records Analyst or designated department, is a violation of copyright law. The following points are to be followed to comply with software license agreements:

1. All users must use all software in accordance with its license agreements and the Sedgwick County’s software policy. All users acknowledge that they do not own this software or its related documentation, and unless expressly authorized by the software publisher, may not make additional copies except for archival purpose.

2. Sedgwick County will not tolerate the use of any unauthorized copies of software or fonts in our organization. Any person illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. All users must not condone illegal copying of software under any circumstances and anyone who makes, uses, or otherwise acquires unauthorized software will be appropriately disciplined.

3. No user will give software or fonts to any outsiders including clients, customers, and others. Under no circumstances will software be used within Sedgwick County that has been brought in from any unauthorized location under Sedgwick County’s policy, including, but not limited to, the Internet, the home, friends and colleagues.

4. Any user who determines that there may be misuse of software within the organization will notify the Software License & Records Analyst, department manager, or legal counsel.

5. All software used by the organization on organization-owned computers will be purchased through appropriate procedures.

I have read Sedgwick County’s Software Compliance Policy. I am fully aware of our Software Compliance Policy and agree to abide by this policy. I understand that violation of this policy may result in my termination.
Appendix C: Security Administrator Agreement
To assure security throughout the entire County network, it is critical that all administrators actively support and fully comply with the measures described in the Sedgwick County IT Security Requirements. An administrator of the County’s Information systems is someone that has any administrator duties on any County information system.
As an administrator of a County information system, you may have access to, and responsibility for, sensitive resources that are connected to the County network and you may be assigned duties that place you in a position of special trust and reliance on your professional integrity. Your job duties may require that you have access to production databases or applications which contain confidential or sensitive information. This information may include personal, financial or Protected Health Information (PHI as defined by the Health Insurance Portability and Accountability Act (HIPAA)).
Administrators of the County information systems shall at all times act in accordance with all applicable laws and County policies, rules and procedures. Administrators shall not use County information systems in an improper or unauthorized manner.
By signing this form, you acknowledge that you will take all steps necessary to protect and maintain the confidentiality, integrity & availability of the information assets you have access to.
I have read the Sedgwick County IT Security Requirements, and I agree to comply with the terms of the policy and of this agreement. Breach of this responsibility may result in personal liability, civil and / or criminal penalties, and may subject me to discipline, up to and including dismissal.
Purpose: This Computer Use Policy establishes policy and procedures applicable to all departments regarding the use of computer technology. These rules and restrictions protect the users as well as the Town. Anyone using the Town’s equipment should be aware of them.

The Town of Bloomfield provides computers, e-mail, and internet access to many of its employees. The purpose of these items is to enable the employees to accomplish the tasks associated with their job descriptions as efficiently as possible. This document explains the rules and restrictions which the Town requires. The purpose of these rules and restrictions is to protect the Town and its computer users, and to insure the safety of the equipment and data.

1. All programs and data residing on the Town’s computers are the property of the Town and as such may be subject to inspection for the purpose of determining compliance to this and other Town policies. This includes data files, programs, application software, documents, e-mail, etc.

2. Computer and network passwords should not be shared. Each person must have his or her own. The employee is responsible for maintaining adequately secure passwords. The name of your spouse or child is not a secure password.

3. Software may be loaded onto Town computers only if its use has been approved by the Information Systems Department and it is licensed by the Town. A license must be purchased (in most cases) for each computer using a given application. You may not buy one copy of a software application and install it on multiple computers unless the license for that software explicitly permits it.

4. Software should not be installed on Town computers without the permission of the Department of Information Systems and Technology.

5. No games other than those included with the operating system should be installed on Town Computers unless they are located in computer labs designed to be used by the public.

6. When new computers are purchased, they will be configured by the Department of Information Systems and Technology. No new computers should be installed without having been through our office. Employees may find security on their new computers is much more stringent than it was on their old ones. Security measures are implemented to protect the Town’s assets. If you feel that the level of security installed on your PC impedes your ability to do your job, discuss it with the Director of Information Systems and Technology and it will be loosened if necessary.

8. If unauthorized data or software is found on a computer, the Department Head will be notified in writing and opportunity given to rectify the problem (e.g. - purchase of software, etc.). If reported unauthorized data or software problems persist and are not rectified, the Town may initiate disciplinary action against the offending employee.

10. Computers or terminals should not be left unattended in a state which affords inappropriate access to records of the Town or otherwise compromises security. Be sure to log out when you leave your workstation for more than a few minutes.

11. The Town purchases and maintains a license for an antivirus program for each computer that it buys. This program must not be inactivated. External files obtained from any source must be scanned for viruses before they are opened.

12. Employees shall provide all passwords or encryption keys for all protected hardware, software, or documents, to the employee’s supervisor prior to use. Employees shall notify their supervisors of their intent to use any other password or encryption to secure computer systems or documents, and explain how and why they intend to use it. Other passwords or data encryption methods may only be used for the purposes of securing information where the information is part of Town business and such passwords or encryption are necessary to protect the information according to Town requirements for confidentiality.

13. Profiles and passwords shall not be posted, disclosed, or shared among multiple people. Information Systems personnel may take any appropriate action to insure sufficient security for computer systems and data. Passwords may be disclosed to Information Systems personnel for Information Systems purposes.
15. It is up to the employees’ good judgment, good faith, and responsibility to police their own content of messages and other forms of electronic communication. E-mail, Internet or any form of electronic communication should not be harassing, libelous, threatening, abusive, foul, or obscene.

16. All disks, tapes, or data obtained from outside the Town computers or networks must be checked for viruses BEFORE they are used in the office. This includes all data obtained by any means or from any source.

17. Unauthorized deletion of any information, data, programs, or software from any computer or computer media is a violation of this policy. Violation of this policy may result in personnel action up to and including termination.

Electronic Mail (E-mail) Use

The Town has established the following policy with regard to access and disclosure of E-mail messages created, sent or received by Town employees using the Town’s E-mail system.

The Town intends to honor the policies set forth below, but reserves the right to change them at any time as may be required.

1. The Town maintains an E-mail system. This E-mail system is provided by the Town and its use is reserved solely for the conduct of business by the Town and its authorized representatives. Incidental personal use of E-mail is permitted on a limited basis.

2. The E-mail system hardware and licensed software are Town property. Additionally, all messages composed, sent, or received on the E-mail system are Town properties. They are not the private property of any employee.

3. The E-mail system may not be used to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

4. The E-mail system may be used to promote Town approved activities and fund-raisers such as the Employees Association, United Way, March of Dimes, Muscular Dystrophy, or other uses that may be approved by the Town Manager.

5. The E-mail system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone’s age, sexual orientation, religious or political beliefs, national origin, or disability.

6. The E-mail system shall not be used to unlawfully send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials. It may be done lawfully if it is specified in the employees’ job description or with prior authorization from the Department Head.

7. The Town reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, sent, or received over the E-mail system for any purpose. The contents of E-mail properly obtained for legitimate business purposes, may be disclosed within the Town without the permission of the employee.

8. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

9. Notwithstanding the Town’s right to retrieve and read any E-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any E-mail messages that are not sent to them. Any exception to this policy must receive prior approval by the Town Attorney.

10. Employees shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Employees should not attempt to gain access to another employee’s messages without the latter’s permission.

11. Some E-mail (both internal and Internet) may be considered a public record and may be subject to public disclosure in accordance with applicable law.

12. Employees who discover a violation of this policy shall notify their supervisor, Department Head, Town Attorney, or Director of Information Systems.

13. Any employee who violates this policy or uses the E-mail system for improper purposes may be subject to discipline, up to and including discharge.

INTERNET USE

Access to the Internet and the use of Internet technologies have become a common means of conducting business. The openness of the Internet and the demands of employees to gain access to Internet...
resources enhance the need to establish guidelines, educate, and raise levels of awareness for all employees involved with Internet technologies. While much of the emphasis is placed on protecting the Town or employee from negative impact of the misuse of the Internet, other important significance is placed on the effective use of the Internet so the Town can achieve the benefits it desires and expects. The primary purpose of Internet access is to support and enhance the information resources and communication capabilities of Town of Bloomfield personnel, and the appropriate sharing of information with other Internet users.

1. Only personnel authorized by the Department Head may post official material on the Internet in behalf of the Town.
2. Postings must not violate any trademark or copyright laws. Any trademarks or copyrighted works used in any Town posted materials must be so noted to include proper credit to the holders of the trademark and copyright.
3. Town Internet facilities are provided to conduct Town business and job related activities. Incidental personal use of the Internet is permitted on a limited basis during breaks, lunch, or after hours. Use of the Internet for personal commercial gain is strictly prohibited.
4. The Town has limited bandwidth in its connection to the internet. Therefore the use of such services as streaming audio or video, downloading of music, and other uses which require high bandwidth are prohibited unless they are required to fulfill some aspect of the employee’s job. Similarly, services such as weather bug which maintain a nearly constant connection to the Internet should not be installed unless necessary for the employee’s job.
5. Software shall not be uploaded or downloaded illegally. It is a serious federal crime.
6. All downloaded files must be checked for viruses before use.
7. Services on the Internet must not be accessed illegally.
8. Employees must not access Internet sites with lewd, obscene, or sexually explicit material.
9. Any employee who violates this policy or uses the Internet for improper purposes may be subject to discipline, up to and including discharge.
INTERNET and E-MAIL CODE OF CONDUCT

Access to the Internet has been provided to staff members for the benefit of the City of New Britain in providing services to the public. It allows employees to connect to information resources around the world. Every employee has a responsibility to maintain and enhance the City of New Britain's public service, and to the Internet in a productive and efficient manner. To ensure that all employees are responsible, productive and efficient Internet users in the performance of public service, the following guidelines have been established for using the Internet.

1. Acceptable Uses of the Internet
Employees accessing the Internet are representing the City of New Britain. All communications shall be for professional reasons. Employees are responsible for ensuring that the Internet is used in an effective, efficient, ethical and lawful manner. Internet Relay Chat channels may be used to conduct official City of New Britain business or to gain technical or analytical advice only. Databases may be accessed for information as needed. E-Mail may be used for business contacts. All messages, even "deleted" information, may be stored and subject to Freedom of Information (FOI) statutes.

2. Unacceptable Uses of the Internet
The Internet shall not be used for personal reasons, including personal gain or advancement of individual gains. Solicitation, accessing or receiving of non-City of New Britain business is strictly prohibited. Use of the Internet must not disrupt the operation of the company network or the networks of others. Use of the Internet must not interfere with employee's productivity. The employee should not leave the E-Mail program open and should log off the Internet when not actively using or away from the workstation. An employee cannot use another person's password or account even with permission.

3. Communications
Each employee is responsible for the content of all text, audio, or images that they place or send or retrieve over the Internet. Fraudulent, harassing or obscene messages are prohibited. All messages communicated on the Internet shall have your name attached. No messages will be transmitted under an assumed name. Users may not attempt to obscure the origin of any message. Information published on the Internet shall not violate or infringe upon the rights of others. No abusive, profane or offensive language is transmitted through the system. Employees may not download or upload any material of derogatory racial content, derogatory religious content, sexual content, political statements, offensive language, any content which would negatively reflect upon the City of New Britain, any material prohibited by law.

4. Software
To prevent computer viruses from being transmitted through the system, software shall not be downloaded without prior authorization. All software downloads shall be downloaded through the Management Information Systems division. Copyrighted materials belonging to entities other than the City of New Britain may not be transmitted by staff on the Internet. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the City of New Britain and/or legal action by the owner of the copyright.

5. Security
All messages created, sent or retrieved over the Internet are the property of the City of New Britain, and shall be considered public information. Therefore, all employees using the Internet should not have any expectation of personal privacy in the use of these systems. The City of New Britain reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications including text and images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

6. Harassment
Harassment of any kind is strictly prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, sexual preference, or any other attribute protected by state and federal law will be transmitted.
7. Violations
Violations of any guidelines are subject to the City of New Britain disciplinary procedures, up to and including discharge. Violators may be subject to loss of access to Internet and E-Mail systems. Violations may also be subject to law-enforcement referrals if laws have been violated.

Electronic mail ("E-Mail") System
Introduction
Computer networks, Internet access, and Electronic mail, popularly known as "E-Mail", are effective and important communication devices in today’s business environment. The City of New Britain has installed a computer network, Internet access and an E-Mail system to provide its employees with this business advantage, and to increase the effectiveness and efficiency of the delivery of public services to the City of New Britain residents.

These technologies are forms of business tools. As such, they are not provided to our employees for any purposes other than business-related needs. The City of New Britain’s computer network, Internet access and E-Mail systems are expensive to install, own and maintain. Unfortunately, they can be misused in a variety of ways, some of which are innocent and others of which are not.

Therefore, in order to maximize the benefits of these technologies or systems to the City of New Britain, the following policy shall govern all use of the system:
Monitoring
It is important for all users of the systems to understand that the City of New Britain, as owner of the systems, intends to monitor their uses to ensure that only appropriate, business-related work and messages are being performed and transmitted.

This monitoring will be performed in a fashion that will permit the City of New Britain to obtain information about system uses and messages, on an ongoing basis, to confirm the systems are functioning properly, and without misuse. Such sampling will also allow the City of New Britain to continually reassess the utility of the systems, and whenever appropriate, make such changes to the systems as deemed fit.

Passwords and Privacy Issues
Employees must understand that the City of New Britain has reserved the right to conduct monitoring of the systems' uses and of E-Mail messages and can do so despite the assignment to individual employees of passwords for systems security.

The passwords are designed to provide systems security from unauthorized users, not to provide privacy to the individual systems users.

The system's security aspects, such as the message delete function for E-Mail and your personal password can be bypassed for monitoring purposes. The City of New Britain's ability to monitor system use and any messages at any time is not restricted or neutralized by these mechanisms. Deleted messages may still be monitored. All messages, even "deleted" messages may be stored and subject to Freedom of Information (FOI) statutes.

Therefore, in addition to the prohibition against personal use found below, employees must be aware that they should not have any expectation of personal privacy in the use of these systems.

Misuse of the systems will result in discipline, up to and including discharge. If necessary to support appropriate disciplinary measures, additional information about personal uses or monitored personal messages will be recorded and provided in confidence to the appropriate department head, supervisor, or manager, or to the personnel office.

Why Monitor System Use or E-Mail?
The systems themselves are expensive for the City of New Britain to install, operate, and maintain. For that reason alone it is necessary to prevent misuse of the systems. However, there are other equally important reasons why the City of New Britain intends to monitor the use of the systems, reasons that support its efforts to maintain a comfortable and pleasant work environment for all employees. Sadly, modern technologies such as the Internet and E-Mail can be used for dangerous and illegal purposes. Experience by other operators of such systems and E-Mail has shown that they can be used for such wrongful purposes as sexual harassment, intimidation of co-workers, threatening of co-workers, breaches of employer, employee or customer confidentiality, copyright infringements, and so on.

Personal Use Prohibited
In order to prevent abusive use of the systems, the City of New Britain will monitor their use and any personal use will not be allowed. To avoid the possibility of observation of personal uses or interception of private personal messages, employees shall not engage in personal uses or send personal messages at any time, to any person.
This means that all users of the systems must restrict themselves to appropriate, business related uses only.

Other Prohibited Uses

Certain specific types of system misuse are expressly prohibited, including but not limited to the following:

* Sending personal messages, of any kind, at any time;
* Sending any form of harassing, threatening, or intimidating message, at anytime to any person (such communications may also be a crime, pursuant to Public Act 95-143, and other laws);
* Gaining or seeking to gain unauthorized access to resources or entities;
* Damaging computers, computer files, computer systems or computer networks;
* Using another person’s password and/or account, regardless of their permission to do so;
* Sending any message that breaches the City of New Britain’s confidentiality requirements;
* Sending any copyrighted material over the system.

In addition, if a particular behavior or activity is generally prohibited, it should not occur in the use of the systems. The City of New Britain reserves the right to amend this policy to include other types of misuse as necessary to maintain proper control over the use of the systems.

Disciplinary Action

Misuse of the systems will result in disciplinary action up to and including discharge.

Complaints of Problems or Misuse

Anyone who is aware of problems, or misuse of the systems should report this to their supervisor, department head, the Director of Management Information Systems, or to the Personnel department. The City of New Britain also reaffirms its commitment to the prevention of sexual harassment in the workplace, and to the principals of affirmative action and equal employment opportunity, and directs individuals who think they have been subject to a violation in these areas to appropriate Sexual Harassment policy or Affirmative Action policy.

Any investigation will be maintained as confidential to the greatest extent possible, while recognizing specific legal requirement to public access to information and the need to investigate thoroughly all complaints.

Implementation

This policy is effective as of May 2001. Monitoring, however, will be delayed a brief time to permit all employees to become fully familiar with the policy, its purposes, and its potential consequences. Systems monitoring will commence on or after May 31, 2001.
Information Technology Policy – Acceptable Use

I. POLICY:
1. Policy: The Kent County Board of Commissioners authorizes the use of the County computer resources for the performance of work and the efficient exchange of information consistent with the County’s statutory, regulatory, and procedural purposes. This policy applies to both networked and stand-alone computer systems.

2. Guidelines: Acquisition, use, operation, and protection of the County’s computing environment shall be conducted in compliance with all applicable laws and regulations, County policies and procedures, and industry best practices.

II. PRINCIPLES:

1. Statutory References: The Kent County Board of Commissioners may establish rules and regulations in reference to managing the interests and business of the County under Public Act 156 of 1851 (MCLA 46.11 (m)).

2. County Legislative or Historical References: The Board of Commissioners adopted an Internet and Online Services Policy to support County tasks with Resolution 2-27-97-22 and Revision I, Resolution 4-22-99-49. Additionally, The Board of Commissioners adopted a Personal Computer Software Policy to enforce copyright and licensing agreements, Resolution 9-25-97-131. This policy supersedes both of these policies. This policy also supersedes the original Acceptable Use Policy, Resolutions 4-27-00-46 and 11-08-01-157.

3. Operational Guidelines – General: Use of the County’s computer resources is a privilege, not a right, and may be revoked at any time for use inconsistent with established procedures and standards. The County owns the hardware and software resources that comprise the County’s computing environment. Data stewardship is the responsibility of the County departments, agencies, or judiciary that generated the data. The County retains the right to monitor and control all access to and activities within the computing environment. Users should have no expectation of privacy when using computer resources.

3.a. Violations of Policy: In the event violations of policy are discovered, these will be brought to the attention of the affected department director and Information Technology director for appropriate corrective action. Any illegal activity will be brought to the attention of law enforcement officials.

3.b. Software Licensing: All software used on County computing resources will be properly licensed to the County. Users will not load or install privately owned software on any County resource. Use of unlicensed software or improperly licensed software is not acceptable.

3.c. Intellectual Property Rights: The County recognizes and respects the rights of intellectual property owners. County computing resources are not to be used to obtain, store, or use illegal copies of copyrighted materials. This prohibition includes, but is not limited to, illegal copies of music, videos, or software.

3.d. Configuration: Users will not perform hardware or software configuration or maintenance on County computing resources. Any configuration / maintenance required will be performed by authorized technical staff.

4. Operational Guidelines – Additional:

4.a. Internet Filtering: In order to promote productive and secure use of County resources, restrictions will be placed on the use of Internet services. Filtering and blocking of Internet sites will be accomplished per the Computing Security Policy.

4.b. Access Authorization and Approval: Access to the County’s computing resources by individuals, whether employees, contractors, vendors, or others, will be permitted pursuant to the Usage Request procedure.

4.c. Authorized County Systems: All County business shall be transacted using only authorized County systems, which include e-mail and other messaging systems.

5. Exceptions: The County Administrator/Controller is authorized to make exceptions to this policy outside those appearing below.

5.a. E-mail Systems: Consultants, contractors, and vendors may use their own e-mail service rather than the County’s e-mail service.
6. Implementation Authority: Upon adoption of this policy, the Board of Commissioners authorizes the County Administrator/Controller to establish any procedures and standards necessary for implementation.

7. Periodic Review: The County Administrator/Controller will review this policy at least every two years and make any recommendations for changes to the Legislative and Human Resources Committee.
County of Kent
Information Technology Policy – Computing Security

I. POLICY: Kent County computing resources will be operated in a manner appropriate for the protection of the information stored and processed in the computing environment. A balance between security and productivity will be established that promotes the security principles of availability, confidentiality, and integrity. This policy applies to all users of County computing resources and all existing and future network connections to and from County and non-County entities.

II. PRINCIPLES:

1. Statutory References: The Kent County Board of Commissioners may establish rules and regulations in reference to managing the interests and business of the County under Public Act 156 of 1851 (MCLA 46.11 (m)).

2. County Legislative or Historical References: Supersedes Information Technology Policy – Network Security, Resolution 7-12-01-84.

3. Operational Guidelines – General: Protection of the County’s computing environment shall be conducted in compliance with all applicable laws and regulations, County policies and procedures, and industry best practices.

   3.a. Connectivity / Access: All requests for external connectivity and / or access to Kent County’s computing environment shall be approved by the Information Technology Director or designee. Remote access required by vendors, consultants, and other non-County entities may require the execution of a Memorandum of Agreement (MOA) or other contractual arrangement.

   3.b. Violations of Policy: In the event violations of policy are discovered, these will be brought to the attention of the department director and Information Technology director for appropriate corrective action. Any illegal activity will be brought to the attention of law enforcement officials.

4. Operational Guidelines – Additional: Information Technology (IT) staff shall take all reasonable steps to make the County’s computing environment as secure as possible. It is the responsibility of County departments, agencies, and the judiciary to provide physical protection for their local systems and the information contained therein.

   4.a. Filtering/Blocking of Internet Sites: In order to promote productive and secure use of County resources, the County Administrator / Controller is authorized to approve filtering and blocking of Internet sites.

   4.b. Network Device Configuration Control: Changes to the configurations of network devices, including but not limited to firewalls, routers, and switches, will be handled only by those personnel designated by the Information Technology director.

   4.c. Network Connectivity / Access: The County Administrator / Controller is authorized to determine and enforce requirements for connections of any devices including, but not limited to, servers, workstations, and external connections to the County’s computing environment.

   4.d. Security Administration: The County Administrator / Controller is authorized to determine and enforce requirements for computing security including, but not limited to, system administration, passwords, account management, and security awareness.

5. Exceptions: The County Administrator / Controller is authorized to make exceptions to this policy.

6. Implementation Authority: Upon adoption of this policy, the Board of Commissioners authorizes the County Administrator/Controller to establish any procedures and standards necessary for implementation.

7. Periodic Review: The County Administrator/Controller will review this policy at least every two years and make any recommendations for changes to the Legislative and Human Resources Committee.
Information Technology Policy – Remote Access

I. POLICY: The Kent County Board of Commissioners authorizes remote access to certain County information systems by County officials and employees upon appropriate approval. Remote access required by vendors, consultants, and other non-County entities will be governed by the Computing Security Policy and may require the execution of a Memorandum of Agreement (MOA) or other agreements.

II. PRINCIPLES:
1. Statutory References: The Kent County Board of Commissioners may establish rules and regulations in reference to managing the interests and business of the County under Public Act 156 of 1851 (MCLA 46.11(m)).
2. County Legislative or Historical References: The Board of Commissioners approved dial-up access by third parties to the County’s computerized Property Tax Administration System in Resolution #5-92-57. The Board of Commissioners also approved specific agreements with six third parties requesting dial up access to the computerized Property Tax Administration System in Resolution #8-12-93-103.
3. Operational Guidelines – General: Use of remote access is a privilege, not a right, which may be revoked at any time. The County retains the right to keep, retrieve and monitor all records of access to County information systems. Use of remote access will be limited to specifically what is required to perform the job and will not include Internet access.
3.a. Violations of Policy: In the event violations of policy are discovered, these will be brought to the attention of the department director and Information Technology director for appropriate corrective action. Any illegal activity will be brought to the attention of law enforcement officials.
3.b. Use of Remote Access: Remote access may be allowed in situations such as the following, but is not limited to these examples:
   3.b.1. To respond to extraordinary circumstances/events on the network in a timely manner;
   3.b.2. To perform emergency maintenance on the network by Information Technology (IT) staff;
   3.b.3. To permit limited connectivity for application processing as requested by the appropriate authorizing individual.
3.c. Approval of Information Technology Director: Before remote access can be established, approval must be obtained from the IT director or designee. The IT director must ensure that the security and integrity of the County’s information systems are maintained, and that the computer system has the capacity and ability to accommodate such requests for remote access.
4. Operational Guidelines – Additional: This policy is intended to allow limited off-site or mobile computing by providing varied levels of access when it is in the best interests of the County to do so.
4.a. Restrictions on Remote Access: Restrictions will be placed on the use of remote access dependent on level and duration of access requested in order to protect the County and its resources.
4.b. Software Licensing: All off-site use of County software will be under proper license in accordance with the County policies.
5. Exceptions: The County Administrator / Controller is authorized to make exceptions to this policy.
6. Implementation Authority: Upon adoption of this Policy, the Board of Commissioners authorizes the County Administrator/Controller to establish any procedures and standards which may be necessary for implementation.
7. Periodic Review: The County Administrator/Controller will review this policy at least every two years and make any recommendations for changes to the Legislative and Human Resources Committee.
Procedures and Standards – Acceptable Use
I. PURPOSE: These procedures and standards, developed at the direction of the County Administrator / Controller, implement the Acceptable Use Policy adopted by the Board of County Commissioners.
II. DEFINITIONS:
A. APPROPRIATE AUTHORIZING INDIVIDUAL: These are individuals, or their designees, who are empowered to authorize access to the County’s computing environment. Appropriate authorizing individuals are as follows:
   A.1. Department Director: The Department Director, Elected Official, or the Chief Judge responsible for the department to whom the employee is assigned in the case of County employees.
   A.2. County Administrator/Controller: The County Administrator/Controller for any non-elected Department Director.
   A.3. Chair of the Board: The Chair of the Board of Commissioners for any Commissioner or the County Administrator/Controller.
B. AUTHORIZATION: All access to the County computing environment requested by County officials, employees, and other entities such as vendors and consultants, must be authorized through the Usage Request procedure; section IV.B later in this document.
C. COPYRIGHTED MATERIAL: Work, typically of a literary, musical, dramatic, or artistic nature, that has been protected by the granting of an exclusive right for publication, production, sale, or distribution.
D. KENT COUNTY SENSITIVE DATA / INFORMATION: Data/information viewable only by the employees of Kent County, or a subset thereof, i.e. payroll, human resources. Though instances may exist where this information is releasable to the public, it is not openly accessible otherwise.
E. MALICIOUS CODE: Computer viruses or other programs purposely introduced to disrupt, damage, or destroy County data and/or information systems.
F. PERSONAL DIGITAL ASSISTANTS (PDA): A family of portable devices offering personal productivity enhancements, particularly certain features of the computer desktop such as spreadsheets, calendars, notes, e-mail, etc.
G. PERSONAL USE: Non-business research and browsing permitted by appropriate authorizing individual. This does not include use for the purpose of shopping, gambling, gaming, nor browsing sites which could fall into the following categories: adult/sexually explicit, violence, criminal skills, hate speech, personals and dating, glamour and intimate apparel, drugs and alcohol, hacking, remote proxies, or weapons.
H. SERVICES: Various methods of information exchange performed over a network, to include but not limited to file transfers, electronic mail, Internet access, telnet, browsing, file and print sharing.
I. USER: Employees, elected officials, judiciary members, interns, volunteers, consultants, contractors, and vendors who access the County’s computing environment to perform services for the County.
J. PORTABLE DEVICES: County-owned or personally-owned equipment that is portable including, but not limited to, laptop computers, tablet computers, personal digital assistants (PDAs), and USB drives (or thumb-drives).
III. STANDARDS: Access to the County’s computing environment is a privilege, not a right. The County owns the resources that comprise the computing environment. Data ownership belongs to the departments, agencies, or judiciary that generate it. The county retains the right to monitor, control, log, audit, or download, without notice, all access to and activity within the computing environment for the purposes of ensuring compliance with policy and monitoring performance. Users should have no expectation of privacy.
A. Violations of Policy: In the event violations of policy are discovered, these will be brought to the attention of the affected department director and Information Technology director for appropriate corrective action. Any illegal activity will be brought to the attention of law enforcement officials.
B. Logon Banners: Logon banners will be used to provide notice to unauthorized users and to advise authorized users of expressed consent to monitoring when logging on to the network. These banners will be loaded onto all systems by technical staff. The banner will be viewable to users from their workstation. Systems which cannot meet these standards will be identified to network security for alternative solutions.
C. Monitoring: Monitoring will be used to identify potential network performance issues, to enforce policy, and to detect intrusion and unauthorized use.

D. Configuration, Maintenance, Software Installation: Users will not perform hardware or software configuration or maintenance on any County computer resources, including the installation of software. Configuration, maintenance, and software installation will be performed by authorized technical staff which includes vendors, contracted personnel, and information technology (IT) staff in other departments, in addition to the IT Department staff. All hardware and software service requests and trouble calls will be reported to the Help Desk or appropriate departmental IT staff.

E. Acceptable Use: All users of the County’s computer resources are expected to conduct themselves in a professional manner, respectful of others and the rights of property, while using computer resources. In addition to the performance of work for the County, the following are authorized uses for the County’s network resources:

E.1. Research/Education: Communication with professional associations, other governments, universities, businesses, and individuals for facilitation of County business, research, and education efforts.

E.2. General Public: Distribution of information to the general public, when such information is provided in accordance with County policies and guidelines for the release of information and the Freedom of Information Act.

E.3. Incidental Communication: Exchanges of information among County employees and professional colleagues that facilitates work assignments and professional discussion in a work-related field of knowledge.

E.4. Personal Use: Users may use computer resources for non-business research or browsing during meal times or outside of work hours, provided they strictly adhere to all other usage policies. Such use must be coordinated and documented with the appropriate authorizing individual prior to being conducted to ensure reasonable limits are set. Limits will be defined, in writing, by either a blanket departmental letter or on a case-by-case letter basis with an information copy forwarded to network security.

E.5. Personal Devices: The use of personally-owned devices that connect to a County-owned computer or network may be restricted if that device creates a conflict with normal use of the computer or network. Examples of such devices include, but are not limited to, memory sticks, flash drives, music/video players, and so on. Personal digital assistants (PDAs) are allowed, but synchronization software must be licensed by the County. Any device requiring non-standard, personally-owned, or unlicensed software to be installed on a County computer is not allowed.

F. Unacceptable Use Standards: No one shall use the County’s computing environment to access sites which may fall in the prohibited categories defined by personal use. No one will use the County’s computer resources for the conduct of the following activities:

F.1. Inappropriate Communication: Sending or receiving communications or material which contains illicit, slanderous, obscene, sexually oriented, racially offensive, religious, threatening and/or discriminatory remarks. Receipt of objectionable, unsolicited material (spam) will not be cause for user access revocation but should be brought to the attention of the IT Department as soon as possible.

F.2. Misuse of Assets: Monopolizing computer resources (i.e., Internet access) through excessive use, causing network and server congestion. Such use detracts from the productivity of others, disrupts network usage, and ties up resources.

F.3. Improper Release of Information: Sending information deemed confidential by the user’s appropriate authorizing individual, or which should not be disclosed under federal, state, or local statute or regulation. If unsure whether the information is releasable or not, check with your supervisor, or FOIA coordinator first.

F.4. Games: Games will not be loaded, installed, or played on the County’s network or computer resources. Games installed by default software setup will be removed before placing the computer on the network.

F.5. Unauthorized Applications: No applications should be used on County computing resources unless they have been approved by the affected department director and the Information Technology director. For departments or enterprise operations with their own technology staff, or departments headed by an elected official, approval can be made by the head of that department / operation solely. This prohibition includes the use of personal copies of legally licensed software as well as programs downloaded from the Internet (“shareware,” “freeware,” scripts, or applets). Unauthorized software will be removed at the discretion of authorized technology staff if, in the opinion of the authorized technology staff member, it is
interfering with proper functioning of any portion of the County’s computing environment or authorized applications.

F.6. Personal Business: Operating a personal business via the County’s computing environment is strictly prohibited.

F.7. Illegal Activities: Engaging in or soliciting illegal activities. These activities include:


F.7.b. Violation of Copyright, License, and Registered Trademark: Downloading, installing, and/or distributing software or data (including music, videos, documents and pictures) with disregard to copyright, license, and registered trademarks. All software and files downloaded on the network will be for direct business use and become County property. They will be properly licensed and registered according to the appropriate software agreement before use. Illegal copies of software or data are subject to immediate confiscation and/or deletion upon discovery.

F.7.c. Computer Crime: Any act to intentionally and without authorization, gain access to, alter, damage, or destroy a computer, computer system, or computer network, or gain access to, alter, damage, or destroy a computer software program or data contained in a computer, computer system, or computer network.

F.7.d. Malicious Code: Intentionally introducing or propagating any virus, worm, Trojan Horse, or other trap-door program code on any computer resources.

F.8. Instant Messaging: Exchanging messages with individuals outside the County’s computing environment via instant messaging applications is prohibited. This practice creates multiple security concerns, and is not necessary for conducting County business. Within the County’s computing environment the use of GroupWise Messenger is encouraged.

F.9. Chatting: The use of Internet web sites or other facilities that allow the use of “chat” is not allowed for other than performing County business. Ordinarily chat will not be used for transactions, but only for obtaining support or information.

F.10. Solicitation: The County’s computing environment is not to be used for mass personal solicitations, including those via e-mail, instant messaging, or broadcast messages.

G. Data Storage: Kent County sensitive data/information will be stored on network servers, not on individual workstations. This will ensure the data/information will be available for backup in the event it is required for recovery purposes. This also ensures the integrity and confidentiality of the information in the event the workstation is removed by unauthorized individuals. Data/information will be stored on its appropriate network drive to prevent sharing of individual user passwords, compromise of user rights and permissions, and/or loss of data/information. Any data, including personal information, stored on local workstations is subject to loss without chance of recovery. Failure to ensure proper data storage is a violation of this procedure.

IV. PROCEDURES:

A. User Identification: Each department will register each of its users with the Information Technology Department in accordance with paragraph II.4.b of the Acceptable Use Policy.

B. Usage Request: Appropriate authorizing individuals will ensure all individuals requiring access read and understand the Acceptable Use Policy and accompanying procedures and standards. Human Resources will ensure all new users sign the Acceptable Use Policy statement during Orientation. Those individuals not attending Orientation will read and acknowledge understanding of the same within their departments and forward the letter via the appropriate authorizing individual to Human Resources. Human Resources will file the original in the appropriate personnel folder and forward an information copy to the Information Technology department.

B.1. User Identification: The name of each user will be registered with the Information Technology Department before establishing access to the County’s computing environment. Health Department, Department of Public Works, and Department of Aeronautics may establish user connectivity to their local area networks in accordance with locally established policy. All users requiring access to the County network will be denied until registration paperwork is received.

B.2. Personal Digital Assistants (PDA): An addendum will be signed by personnel wishing to use a PDA. Only after receiving the signed addendum with the service request will a PDA be configured to work in the County’s computing environment. Individuals refusing to sign the statement will be denied access and the matter will be turned over to Human Resources for resolution.
B.3. Remote Access to GroupWise: GroupWise provides remote access to e-mail and calendaring through an Internet connection. Department directors will approve requests on a case-by-case basis using the Remote Access to GroupWise attachment. If made available to hourly employees, directors will determine if compensation should be made for accessing the system remotely.

C. User Responsibilities: It is the responsibility of all users to protect the computer resources they use and the information contained both on their workstation and on the network. All users will comply with the following:

C.1. Passwords: These will be uniquely assigned by each user and should not be provided to or shared with coworkers, supervisors, or other individuals. Users should not write down passwords. Additionally, users should not construe passwords as a means to create secure communications; they are merely a way to identify and authenticate you to the computer and/or network.

C.2. Unattended Terminals: If a terminal must be left unattended for any amount of time, a screensaver protected by a user-defined password will be used.

C.3. Information Security: Be wary of requests for information or access to your workstation by outside individuals. “Social engineering,” or tricking unsuspecting individuals into giving information about their system, is a very real threat. If the request seems unusual, check with a supervisor first. Never give system information over the phone unless you know the individual calling you.

C.4. Anti-virus Software: Ensure anti-virus software on your computer is enabled, working, and your computer is receiving updates. All viruses detected will be reported to the local system administrator and the County Network Security Administrator.

C.5. Signature Line: All e-mail sent to recipients outside of County resources must contain a signature line with the following information: user’s name, department, and telephone. Additionally, the following statement must appear: “This message has been prepared on resources owned by Kent County, MI. It is subject to the Acceptable Use Policy of Kent County.”

C.6. Wireless Devices: All users of wireless devices must be aware of the security implications. Wireless access (typically identified as “Wi-Fi”) is often an unsecured method of communication. Precautions for using wireless access are constantly changing, and users are urged to contact the Information Technology department before utilizing wireless access for any County purpose or on any County equipment.

C.7. Portable Devices: As described in J. under Definitions. Loss of a County-owned portable device will be investigated and, depending on circumstances, disciplinary action may be taken. Confidential or sensitive information should not be stored on portable devices due to the risk of loss or theft (refer to III.G.). Users storing any information on a portable device must work with the Information Technology department so that appropriate backup and encryption procedures are available.

C.8. Confidential / Sensitive Data: All users have a responsibility to insure that confidential and / or sensitive data is reasonably protected. In particular, that means that confidential or sensitive data will not be copied onto personal devices or onto home computers via a remote connection to the County. See also C.7 above, Portable Devices regarding data encryption.

D. Software Licensing: All software installed on County computing equipment shall be properly licensed. The Information Technology department, in conjunction with the Purchasing department, shall track and file all software licenses. Exceptions for software license tracking will be made upon receiving a written request from a department director. To ensure County compliance with licensing requirements, the Information Technology department will conduct periodic audits of software installed on County computers. In the event unlicensed software is detected, department directors will be contacted to determine if they will purchase a license or the software is to be removed.

E. Security Awareness: All users will participate in the Security Awareness Program. Directors will ensure user participation and follow-up on their departments in compliance with established procedure to ensure 100% coverage.

V. DISTRIBUTION: These procedures and standards will be distributed upon adoption by the County Administrator/Controller’s Office to County departments, agencies and the judiciary.

VI. PERIODIC REVIEW: These procedures and standards will be reviewed at least every two years by the Information Technology Department director, with recommendations forwarded to the County Administrator/Controller.

Each user must complete, sign, and return to the Human Resources Department

ACCEPTABLE USE REQUEST AND ACKNOWLEDGEMENT

4/7/2008
I ____________________________________ (print name) hereby request access to the Kent County computer system. I acknowledge that I have read and understand the Acceptable Use Policy, with accompanying Procedures and Standards, and agree to comply with their terms and conditions. Any data generated by my computer activity is owned by the respective department, agency, or judiciary.

I acknowledge that Kent County reserves the right to monitor all of my system activity in accordance with the provisions of the Acceptable Use Policy, Procedures, and Standards, and I further acknowledge that I have no reasonable or legitimate expectation of privacy or security in my use of the system. I understand that any violations of the Acceptable Use Policy, Procedures, and Standards may result in disciplinary action in accordance with the County’s Personnel Policies.

Each user approved to use a PDA must complete, sign, and return this addendum to the Information Technology Department

ADDENDUM FOR PERSONAL DIGITAL ASSISTANTS

I ____________________________________ (print name) hereby request use of a personal digital assistant (PDA). The PDA will be synchronized to my Kent County computer system. I acknowledge that any County information generated or synchronized on my PDA is owned by my respective department, agency, or judiciary. This information will be removed upon my termination of employment, whether voluntary or involuntary.

I will observe the following security precautions regarding PDAs:

1) A separate, unique password, not associated to my account(s) or workstation will be used.
2) Anti-virus scans will be performed on any information before synchronizing it to the PDA.
3) The “Turn Off & Lock Device” feature will be used to prevent any unauthorized use.
4) The “Beam Receive” will be enabled only as necessary to prevent receiving unwanted information.
5) Monitor the HotSync Log and Last HotSync Operation date to ensure no unauthorized HotSync operations were performed.
6) Keep constant vigil on the physical location of the PDA to prevent theft and loss of information.
7) Report all suspected or known tampering with the PDA or any physical loss of the device and the information contained therein.

I understand that any violations of the Acceptable Use Policy, Procedures, and Standards may result in disciplinary action in accordance with the County’s Personnel Policies.

Each user approved to use GroupWise remotely must complete, sign, and return this addendum to the Information Technology Department.

ADDENDUM TO REMOTE ACCESS FOR GROUPWISE

I ____________________________________ (print name) hereby request Remote or Web Access to the Kent County GroupWise email and calendaring system. I acknowledge and agree to comply with the following terms and conditions. I further understand that the Acceptable Use Policy does hereby govern all Remote Access and that violation of these terms and conditions may result in disciplinary action in accordance with the County’s Personnel Policies.

TERMS AND CONDITIONS

1) I acknowledge that my access does not constitute telecommuting, nor can it be construed as authorized work for the County. My access to GroupWise is strictly for my convenience and I will not let other individuals use my e-mail account for any purposes.
2) The County makes no representation that all privately owned computer hardware or software will work with the GroupWise application.
3) The Help Desk will provide technical support for GroupWise software settings only. Please do not ask the Help Desk for assistance with privately owned computers, peripherals, or other software.
4) Users should be aware that it is possible to download a virus to their home computer using remote access. The end-user assumes all risks, but should consider running virus protection software on their computer.
5) While GroupWise Remote Access will generally be available 7 days a week, the County makes no specific warranty that GroupWise Remote Access will always be available at any specific point in time.
6) Users must realize that communications sent via the Internet is not necessarily protected from viewing by others.
7) The purpose of this Remote Access is to facilitate communication and convenience. It is a privilege and not a right. Inappropriate use may result in cancellation of these privileges as well as disciplinary action.

4/7/2008 Page 166 of 296
Procedures and Standards – Computing Security

I. PURPOSE: These procedures and standards, developed at the direction of the County Administrator / Controller, implement the Computing Security Policy adopted by the Board of County Commissioners.

II. DEFINITIONS:

A. AGING LENGTH: The length of time that must elapse before a particular password can be used again by the same user.

B. APPROPRIATE AUTHORIZING INDIVIDUALS: These are individuals, or their designees, who are empowered to authorize access to the County’s computing environment. Appropriate authorizing individuals are as follows:

B.1. Department Director: The Department Director, Elected Official, or the Chief Judge responsible for the department to whom the employee is assigned in the case of County employees

B.2. County Administrator / Controller: The County Administrator/Controller for any non-elected Department Director.

B.3. Chair of the Board: The Chair of the Board of Commissioners for any Commissioner or the County Administrator/Controller.

C. AUTHORIZATION: All access to the County computing environment requested by County officials, employees, and other entities such as vendors and consultants, must be authorized through the Usage Request procedure; section IV.B of the Acceptable Use Procedures.

D. BEST EFFORTS BASIS: Situations where insufficient prior notice has been given for Information Technology staff to research and respond to requests for service. In such circumstances IT staff will do their best to accommodate the late requests but will do so after existing commitments and priorities have been fulfilled. Results cannot be guaranteed in these circumstances.

E. BRUTE FORCE CRACK: A process of guessing passwords, normally automated by a program, that will try every conceivable character combination until the password is revealed. The process is associated with hacker activity because it does not test the strength of passwords, it reveals them.

F. DENY STANCE: A restrictive attitude with respect towards security in which one specifies what services will be allowed and prohibits all others.

G. FILTERING: A process of permitting access to only specified hosts and ports. It also applies to the filtering out or blocking of unacceptable Internet sites.

H. FIREWALL: A network device used to provide a layer of defense from outside sources.

I. LEAST PRIVILEGE: The most fundamental principle in security of providing only the privileges, rights, and resources required to do the job and nothing more.

J. NETWORK SCAN: An examination of the network and its hosts for the purpose of identifying what services are available and what security vulnerabilities exist which may be exploited.

K. REMOTE ACCESS SERVER (RAS): A network device used to provide remote users with access to their networks, usually unencrypted.

L. RULES OF ENGAGEMENT: The written, agreed upon conditions under which a network scan may be performed by Information Technology staff.

M. SERVICES: Basic network resources, such as a mail, ftp, etc. which are located on all networks, usually represented by a corresponding port number.

N. VIRTUAL PRIVATE NETWORK (VPN): A secure, encrypted remote access connection created within an already existing network, usually the Internet, which provides the functionality as if the user were logged on locally to the network.

III. STANDARDS: Kent County will conduct computing security from the deny stance. Everyone who uses County computing resources, in any manner, has responsibilities for computing security.

A. Responsibilities:

A.1. Appropriate Authorizing Individual: A key responsibility performed by this individual is identifying what access rights and permissions to the various systems are required by their personnel in the performance of their daily jobs. To this end, this individual will conduct and document an annual review of users’ rights and permissions with the appropriate system administrator’s aid. The review will ensure that the proper access levels for the user groups are set and that all systems, databases, etc. required for work can be accessed by department personnel.
A.2. System Administrators: All system administrators will be identified, in writing, by the appropriate authorizing individual. Both primary and alternate system administrators will be designated for each server. System administrators will be held responsible for the host security of the systems under their control.

A.3. Users: User responsibilities are identified in the Acceptable Use and Remote Access policies. User responsibilities extend to the protection of information and resources they have access to in the course of their job and compliance with County policies.

B. General Computing Security

B.1. Passwords and Accounts: Password and account management are basic tools for enforcing security.

B.1.a. Password Management: Password management should be performed using the following minimum standards:
- Change Frequency: Every three (3) months
- Aging Length: Eighteen (18) months
- Composition: 7 characters in length, using a combination of alphanumeric and special characters

Exceptions to this standard shall be reported to the IT department. System administrators shall not force the use of system-generated passwords. System administrators are authorized to test password strength and policy compliance; however, brute force cracks shall only be used in order to recover passwords on servers. All other use of brute force cracks will be viewed as malicious activity and may be cause for disciplinary action.

B.1.b. Account Management: The Human Resources Department, Department and Agency Directors, and the Judiciary will keep the IT Department and appropriate local system administrators informed of all personnel actions (new hires, temps, contractors, vendors, transfers, and terminations) in order to provide proper user account management. System administrators will release account information for terminated users to the appropriate director to determine the disposition of files. Department Directors will have 30 days to review and decide on the disposition of the files. After 30 days, the account and any remaining associated files will be deleted by the system administrator.

B.2. Network Device Configuration Control

B.2.a. Service Requests: Configuration of all firewalls, routers, switches, hubs and other network devices will be controlled and changed through a written or electronically submitted service request. Prior coordination of changes will occur in sufficient time for the network analyst to respond to the request.

B.2.b. Change Log: Changes to configuration will be recorded in a change control log after the change is made.

IV. PROCEDURES:

A. Network Device Configuration Control

A.1. Service Requests: Configuration of all firewalls, routers, switches, hubs and other network devices will be controlled and changed through a written or electronically submitted service request. Prior coordination of changes will occur in sufficient time for the network analyst to respond to the request.

A.2. Change Log: Changes to configuration will be recorded in a change control log after the change is made.

B. Filtering / Blocking of Internet Sites

B.1. Management of Filter: The County Administrator/Controller will provide written authority to the Information Technology department for those categories of sites to be blocked. IT staff will maintain the site blocking application and make changes as requested. Changes can be requested for individuals to access specific sites by their appropriate authorizing individual. Removal of sites from filtering for everyone will be requested by the Information Technology director after a site review.

B.2. Reporting: Requests for Internet monitoring reports will be addressed to the Information Technology director by the appropriate authorizing individual. In the director’s absence, the County Administrator/Controller may request the preparation of specific reports.

C. Network Connectivity and Access: Users should not connect devices, whether County-owned or personally-owned, directly into the County’s network without first contacting the Information Technology department. Departments with their own IT staff may connect devices to their own local networks provided the devices will not adversely affect the County’s overall network or configuration. Failure to notify either County IT staff or local IT staff prior to connecting a device to a County network may mean the device will not operate properly or adversely affect other devices on the network. IT staff will assist on a best efforts basis in situations where no prior notification occurred.
C.1. Non-County Entities: All non-County entities will be required to complete an Interconnection Request Document as a feeder document to a Memorandum of Understanding (MOU). Issues of support, access, connectivity, and security will be addressed to delineate both parties’ responsibilities involved in the connectivity. Each MOU will be site specific. Violations of the MOU may result in connectivity termination. Resolution of these breaches must be satisfactorily agreed upon by both parties, in writing, before communications is restored.

C.2. Access Control: Access to the County network will be controlled through appropriate mechanisms, which are subject to change. These mechanisms will be specified and controlled by the Information Technology department.

C.2.a. Filters and Authentication: Two factor authentication will be used whenever possible through the use of SecureID tokens. Filtering of user accounts will be accomplished to ensure least privilege access. When connecting via the VPN concentrator or RAS, Internet access will be prohibited.

C.2.b. Modems: Connection via modem directly to the County’s network is not supported. The only exception will be those existing connections which are grandfathered until they can be phased out.

C.3. Dual Network Connections: Accessing both a secure connection to the County’s network and a connection to an outside network simultaneously is prohibited. This could happen, for instance, by using a laptop computer that is at the same time connected via a cable to the County’s network and via a wireless connection to an outside network. An exception will be made for public safety equipment, where such dual connections may be necessary in an emergency.

D. Network Scans / Packet Captures

D.1. Network Security Assessments: Network Security will perform scans of all zones, which will be performed under strict written and agreed upon rules of engagement from the Information Technology director. Reports of these scans will be made available to the appropriate manager for dissemination. A courtesy copy will be provided to the Information Technology director and the Deputy Director for Technology. Upon written notification of corrective action(s) being applied or after 30 days of initial reporting, rescans will be performed to ensure the appropriate fix action was implemented effectively.

D.2. Additional Scans or Packet Captures: Other County or departmental IT staff may perform scans or packet captures provided formal, written authority is provided and rules of engagement are established and strictly followed. Reports will be generated in all cases where vulnerabilities are uncovered. These will be provided to Network Security for investigation and verification.

D.3. Unauthorized Scans and Packet Captures: Any scans or packet captures performed without formal written authority will be classified as hacker activity and reported to the Information Technology director, and the appropriate authorizing individual for possible disciplinary action.

V. DISTRIBUTION: These procedures and standards will be distributed upon adoption by the County Administrator/Controller’s Office to County departments, agencies and the judiciary.

VI. PERIODIC REVIEW: These procedures and standards will be reviewed at least every two years by the Information Technology Department director who will make recommendations to the County Administrator/Controller for any amendments.
Procedures and Standards – Remote Access

I. PURPOSE: These procedures and standards have been developed at the direction of the County Administrator / Controller, to implement the Remote Access Policy adopted by the Board of County Commissioners.

II. DEFINITIONS:

A. APPROPRIATE AUTHORIZING INDIVIDUAL: The person who may authorize the use of remote access by a user. These individuals are specifically defined as follows:

A.1. Department Director: The Department Director, Elected Official, or the Chief Judge responsible for the department to whom the employee is assigned will be the appropriate authorizing individual for all County employees.

A.2. County Administrator/Controller: The County Administrator/Controller will be the appropriate authorizing individual for any non-elected Department Director.

A.3. Chair of the Board: The Chair of the Board of Commissioners will be the appropriate authorizing individual for any Commissioner or the County Administrator/Controller.

B. AUTHORIZED USER: Refers to any County official, employee, contractor, or other individual approved to access County information systems by the appropriate authorizing individual.

C. HOST SYSTEM: The computer system to which the remote user will connect.

D. REMOTE ACCESS: The use of a County computer system from an off-site location.

E. SECUREID TOKENS: A small device that displays a changing number. The devices are used with a password to establish authentication of users wanting to remotely access County computing resources.

F. USER SYSTEM: The computer system from which the remote user will connect.

III. STANDARDS:

A. Acceptable Use Standards: Acceptable uses for Remote Access will include, but not be limited to, the following:

A.1. File Transfers: Sending and receiving data files. The files must be scanned for viruses before being uploaded and immediately after download.

A.2. Information Processing: Accessing software programs and data on the host system to add, delete, or modify records and files.

B. Unacceptable Use Standards: Unacceptable use of Remote Access includes any use in violation of the Employee Code of Conduct Policy while accessing County computer systems. Internet access while using the County’s network via Remote Access is prohibited. Other unacceptable uses for Remote Access will include, but not be limited to, the following:

B.1. Personal Use: Use not related to the conduct of work on behalf of Kent County.

B.2. Unauthorized Users: Users will not let anyone, including family members, use their access privileges and will report any unauthorized access, known or suspected, to their department director and the Network Security Administrator.

C. Consequences of Unacceptable Use: Any unacceptable use may subject the authorized user to disciplinary action, up to and including termination of employment.

IV. PROCEDURES:

A. Remote Access Authorization and Approval: Requests for remote access will be handled in a two step process, authorization and approval. Departments with their own IT staff will be required to coordinate with the County’s IT department when providing any direct remote access to their local network. This coordination will ensure appropriate security safeguards are implemented and associated risks to the County’s network are minimized.

A.1. Authorization: All remote access to County computer systems requested by County officials and employees must be authorized by the appropriate authorizing individual.

A.2. Information Technology Department Director’s Approval: Requests for remote access to the County’s computer system must be approved by the Information Technology director or designee. Requests for access must be submitted using the form attached to this Procedure. The Information Technology Department director will forward the request to the appropriate staff for action upon approval, or submit a written statement containing the reason for denial to the appropriate authorizing individual.
A.3. Coordination with Information Technology Director: Departments with their own IT staff may grant direct remote access to their own local area network (LAN). In these cases, because their network is connected to the County’s, coordination between the appropriate director and the County IT director will take place prior to granting remote access. This coordination will ensure the identity of any outside agency connecting to the LAN in question is known by the County, the services provided to the remote user, and how long this type of access will be required (one-time, periodic, full-time). The intent is to ensure appropriate changes are made and network security is maintained for the County’s computing environment.

B. Department Director Discretion: Department directors will determine if the benefit of remote access justifies the use by an employee or outside agency.

B.1. Approvals: For non-exempt employees, the department director or designee must approve all work performed offsite. Performance of unauthorized work off site may subject the employee to disciplinary action.

B.2. Measurement: If more than a minimal amount of work is performed, the employee’s department director should ensure some measurement of performance is used.

C. Determinants for Use

C.1. Access Required to Conduct County Business: If the appropriate authorizing individual requests remote access for the performance of job functions or to conduct County business the cost of purchasing the necessary equipment, software (including virus protection), network connections, SecureID tokens, and other expenses will be incurred and borne by the requesting department.

C.2. Host Equipment and Software: The appropriate authorizing individuals will ensure that all remote access users have the appropriate equipment and software versions to connect to the host system. The Information Technology department will determine the level of access needed to connect to the host system, with input from the requesting department director.

C.2.a. User Equipment: The appropriate authorizing individual will budget for and provide the necessary equipment to access the County’s computer system from a remote location when required to conduct County business. Department directors may allow the user to use new or existing equipment. Equipment and SecureID tokens will be returned upon request. Damage to or loss of County-supplied equipment will be investigated and may result in disciplinary action.

C.2.b. User Software: The appropriate authorizing individuals will budget for and provide the necessary software (including virus protection) to ensure compliance with software licensing and copyright for those users who have been authorized to use Remote Access. Users are required to return County-owned software.

C.2.c. Additional Costs: Costs for connectivity charges incurred by users for remote access will be reimbursed by the County only when prior approval has been granted and costs are budgeted for by the appropriate authorizing individual.

C.3. Virus Protection: The appropriate authorizing individuals must ensure that all equipment used for remote access is protected by virus protection software which is updated on a regular basis. If such software is found to be outdated or insufficient to protect County-owned software, hardware, or data, the user’s remote access to the County network will be disabled immediately.

D. User System Installation: Remote access users are expected to have full knowledge of the use and operation of the necessary software and equipment, including software installation and equipment set-up.

E. Inspection of Facilities and Equipment

E.1. Safety: Authorized County personnel will have the right to inspect off site locations to ensure compliance with applicable safety standards.

E.2. Appropriateness: Information Technology staff or other authorized County personnel will have the right to inspect equipment for appropriate capacity, proper installation, and effective virus protection.

F. User System Support: Equipment and software purchased with County funds for remote access and provided as a requirement to conduct County business will be supported by the County’s Information Technology Department. This support will be in the form of Help Desk access during regular business hours, and software installation, training, and equipment set-up demonstration with Information Technology Department staff. All equipment and software problems will be addressed through the Information Technology Help Desk only if the equipment and software are delivered to the Information Technology Department or its designee.
G. Acceptance of Policy: Before receiving remote access, each authorized user will sign a statement certifying that s/he has been granted Information Technology Department director approval and understands and will abide by provisions contained in the Policy, Procedures and Standards.

V. Review for Continuance: Each instance of remote access will be established with an expiration period. The initial approved period of access will not exceed 90 days. Within 30 days of expiration, a review for continuance will be conducted to ascertain whether or not the need still exists for remote access. Department directors will be advised via e-mail if any personnel are affected. Unless the notification is returned verifying need for extension of this service, the access will be terminated. Extension requests must cite reason for extension and period of extension required.

VI. DISTRIBUTION: These procedures and standards will be distributed upon adoption by the County Administrator/Controller's Office to county departments, agencies and the judiciary.

VII. PERIODIC REVIEW: These procedures and standards will be reviewed at least every two years by the Information Technology Department or its designee, with recommendations forwarded to the County Administrator/Controller.

Each user seeking to remotely access the County’s network must complete, sign, and return this addendum to the Information Technology Department.

ADDENDUM TO REMOTELY ACCESS KENT COUNTY’S NETWORK

I ____________________________________ (print name) hereby request Remote Access to Kent County’s network. I acknowledge and agree to comply with the following terms and conditions. I further understand that the Acceptable Use, Computing Security, and Remote Access Policies do hereby govern all Remote Access and that violation of these terms and conditions may result in disciplinary action in accordance with the County’s Personnel Policies.

TERMS AND CONDITIONS

1) I acknowledge that my access does not constitute telecommuting, nor can it be construed as authorized work for the County. My access to the network is strictly for my convenience and I will not let other individuals use my e-mail account for any purposes.

2) The County makes no representation that all privately owned computer hardware or software be able to connect remotely to the County’s network.

3) The Help Desk will provide limited technical support for remote connections. Please do not ask the Help Desk for assistance with privately owned peripherals or software other than that supplied for the remote access.

4) Users should be aware that it is possible to download a virus to their home computer using remote access. The end-user assumes all risks, but should consider running virus protection software on their computer.

5) While Remote Access will generally be available 7 days a week, the County makes no specific warranty that Remote Access will always be available at any specific point in time.

6) While we take reasonable security precautions, users must realize that communications sent via the Internet is not necessarily protected from viewing by others.

7) The purpose of this Remote Access is to facilitate communication and convenience. It is a privilege and not a right. Inappropriate use may result in cancellation of these privileges as well as disciplinary action.
To provide definitions and clear guidelines, policies and procedures to employees regarding the security of Bradford County's information assets.

Background
Information has become a vital resource of the County and is critical to the day-to-day operation of the County. Bradford County maintains a great deal of information, much of which is protected by federal or state statute. This information, like any other asset, must be protected from release to unauthorized personnel.

Scope
The variety of computing and electronic communication access and tools that the County provides its employees include but are not limited to desktop, laptop, mobile and central computers, internal and external networks, electronic mail (e-mail), Internet, modems, and facsimile systems. These tools are County owned and publicly funded; the computer systems and the software information contained on or conveyed through them are the property of the County. Access and use are restricted by these Computer Policies and Procedures. Equipment that is the property of another entity, but used by County employees in the course of their work, is also encompassed in this policy. Telecommunications and Commonwealth of Pennsylvania computer systems and networks are not included in this policy.

By addressing the issues of use for computer communications, the County ensures maximum benefits by recognizing a critical and defined balance between the need for open communications and the protection of County assets. Each system may, at times, have its own set of policies and procedures. In those cases where communications are carried across other regional networks or the Internet, employees of the County are advised that the most restrictive and security conscious policies takes precedence over acceptable use policies of those other systems.

Audience
This document is intended for use by Bradford County Supervisors who are responsible for County Information assets.

Responsibilities

Commissioners
* Establishes the County's policies for information security, computer hardware and software.
* Reviews capital expenditure requests for computer hardware and software and ensures that they are justified in accordance with the Purchasing Hardware and Software policy statement.

Information Technology (IT) Department
* Recommends the purchase and installation of hardware to support the connection of computers to the County's mainframe computer(s) and/or networks.
* Reviews the use of hardware and software throughout the County to ensure effective use of the County's resources.
* Recommends policies for computer hardware and software to Commissioners.
* Develops procedures to implement the County's policies.
* Recommends software and application systems to be used on the County's computers.
* Recommends hardware to be used by the County.
* Provides consultation and assists in the selection and the installation of computer hardware and software for all departments of the County.
* Evaluates equipment and recommends standards.
* Evaluates and recommends general purpose software. Assists departments in evaluating application and special purpose software.
* Upon request of department heads, elected officials or Commissioners; evaluates the training needs of departments and assists in the formulation of specific training programs for appropriate personnel. Develops in-house training where appropriate and develops a recommended list of external training programs.
* Coordinates and tracks maintenance and repair of computer equipment on behalf of Bradford County.
* Maintains and controls a reference library.
Physical Security of Information Assets

Data Classification

It is essential that all County data be protected. However, there are gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. Bradford County recognizes three classes of data that are described below.

High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as but not limited to HIPAA, Drug and Alcohol, and CYS are in this class. Payroll, personnel, and financial information are also classified as High Risk because of privacy requirements.

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the County if disclosed or modified. The data owner should make this determination. It is the data owner’s responsibility to implement the necessary security requirements.

Confidential – Data that would not expose the County to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner’s responsibility to implement the necessary security requirements.

Public - Information that may be freely disseminated. However, even though the data may be freely disseminated to the public, the integrity of the data must be protected.

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the County.

* Data owners and their supervisors must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

* No County-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.

* Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification and to any applicable statute.

* All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

* Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Data Security Policy

County Information Assets will be handled in accordance with their Data Classification and in accordance with appropriate federal and state statutes and regulations.

Bradford County employees may be in a position to receive confidential information during the performance of their duties. County employees shall never use information obtained confidentially for any purpose and shall respect the privacy of individuals. Since public access of information varies, employees should consult with their supervisor/department head regarding the dissemination of privileged information. Violations of this confidentiality requirement will be grounds for disciplinary action, including dismissal.

Document Security

Network Printing

When users are printing High Risk and Confidential data they will take precautions to ensure that their privacy and security are protected. Examples of this include

1. Standing by the printer while the job is printing.
2. Immediately remove the documents from the printer.
3. Print to a printer/copier mailbox and release the print job when standing at the printer/copier.

File Cabinets and Record Rooms

1. File cabinets that contain High Risk and Confidential Data will be kept locked at all times.
2. File Rooms will remain locked when unattended.

Data Transmission & Encryption Policy
High risk data must be encrypted during transmission over insecure channels. An insecure channel is defined as any public network, including but not limited to the Internet. The Public Switched Telephone Network is considered to be a secure medium. Confidential data should be encrypted during transmission over insecure channels. Bradford County Employees are not permitted to encrypt or apply passwords to data unless it is for the purpose of transmission over an insecure channel.

Information Security Officer
The County will appoint an Information Security Officer who is responsible for implementing and monitoring a consistent data security program. The Information Security officer will:
1. Assume responsibility for determining appropriate security measures and creating policies and procedures that monitor and control access to County Information Resources.
2. Update security standards as necessary.
3. Take responsibility for the prevention, detection, containment and correction of security breaches.
4. Coordinate information security activities with each section of the organization including human resources, information systems and physical security.
5. Monitor security activities and oversee the application of specified security procedures.
6. Assist personnel in assessing data to determine classification level.
7. Implement a security awareness program.
8. Provide assistance for information security throughout the organization.
9. Review security violations and follow reporting procedures.

Risk Assessments and Risk Management
Bradford County will hold annual risk assessments that may be conducted by County employees, external consultants, or a combination thereof. The results of risk assessments will be used to create annual risk management plans that will identify and quantify risks and recommend actions to mitigate those risks. The Information Security Officer is responsible for ensuring that risk mitigation is assigned to appropriate parties and completed within a reasonable amount of time.

Data Retention Policy
County Information Assets will be retained in accordance with applicable federal and state statute. Where permitted by statute, documents will be scanned, indexed, and retained in electronic format as a substitute for original documents.

Server Security
Servers will be placed in locked rooms that have limited access to authorized personnel only. Administrative access to servers will be strictly limited to members of the IT department and approved contractors. When possible, servers will be placed so that only IT members and IT contractors have access to them. Because of privacy and security requirements only IT or approved contractors may receive administrative-level permissions.

For departments or facilities with 24-hour operations, staff members who are not employed in the IT Department may require the ability to perform some administrative-level tasks. A user requiring this ability will be granted administrative control of his or her Organizational Unit only and will be granted “Server Operator” status.

Server Desktops will remain logged out or locked at all times unless a member of the IT staff or a contractor is working on the server. When administrative tasks are complete, the operator will log out or lock the server immediately.

When remote access to servers is required, members of the IT Department will use only approved, encrypted communications for these sessions.

Server File System Security
With the exception of HOME and MAIL folders, only Active Directory Groups will be used to apply security to server resources on Bradford County servers. Individual users will not be assigned access to any folders or other shared server resources.

Home Folders
Users who are assigned network accounts will receive a HOME directory (folder) for storage of their daily work. Only the individual user, DH_department_GROUP and the MIS_GROUP will have access to HOME folders.

Mail Folders
Users who are assigned internal email accounts will receive a MAIL directory (folder) for storage of their emails. Only the individual user, DH_department_GROUP and the MIS_GROUP will have access to MAIL folders.

Shared Directories
Users will be assigned access to shared folders in accordance with departmental or workgroup requirements as directed by the user’s supervisor. Shared folders are for the purpose of allowing entire workgroups or departments to share data. Requests for special workgroups or cross-departmental workgroups should be referred to the IT department.

Application Folders
Users will be assigned access to shared folders in accordance with departmental or workgroup requirements as directed by the user’s supervisor.

Active Directory Groups
The following guidelines will be used when setting up active directory groups to apply security to servers and computers connected to the Bradford County network.

MIS_GROUP
Personnel in the IT Department will belong to this group. This group will have administrative rights to the servers and computers connected to the network.

RDP_server_GROUP
Each server will have its own “RDP_server” group. This group will be placed on each server for remote access of the server. A user who needs to access a server remotely would be placed within this group and removed once the need no longer applies.

WS_server_GROUP
Server in “WS_server will be replaced with the server the user of the workstation has his HOME folder on. This group will be placed on each workstation connected to the network and will have administrative privileges to that workstation. A user who needs administrative rights to a workstation will be temporarily added to this group and removed once the need no longer exists.

ADMIN_server_GROUP
Each server will have its own “ADMIN_server” group. This group will be placed on each server connected to the network and will have administrative privileges to that server. A user who needs administrative rights to a server will be temporarily added to this group and removed once the need no longer exists.

DH_department_GROUP
Each department of Bradford County will have its own Department Head group. This group will be given access to a department’s folders and all subfolders. This includes HOME and EMAIL folders associated with the department. Department heads as well as any other managerial staff deemed appropriate by the department head will be a member of this group.

Department_GROUP
Each department of Bradford County will have its own departmental group. This group will be given access to the department’s folder and any shared subfolders. Employees within the department with network accounts will be members of this group.

Application
Each application being used by multiple departments will have its own application group. This group will be given access to an application’s data. Users of the application will be members of this group.

Support
Each vendor that supports a software application will have a support group. This group will be added to WS_server, ADMIN_server and/or Application group on an as needed basis.

Critical Systems, Applications and Data
Safety Critical Systems & Applications (SCS)
This is a computer, electronic or electromechanical system whose failure may cause injury or death to human beings. Downtime is unacceptable and appropriate measures, such as redundant systems are required.

During an emergency, these systems will receive the highest priority and will be restored as quickly as possible.

These systems will maintain uptime of 99.7% or better.

Mission Critical Systems & Applications (MCS)
This is a computer, electronic, or electromechanical system whose failure would cause grave financial consequences. Downtime during general business operations is unacceptable. However, downtime
during an emergency or disaster is acceptable if the system assumes operations within a period of 48 hours after the emergency is over. These systems will maintain uptime of 99% or better.

Core Systems & Applications (CS)
This is a computer, electronic, or electromechanical system whose failure would cause operational difficulties, increased workload, and inconvenience to staff and clients. These systems will maintain uptime of 98% or better.

During an emergency, operations and data should be restored within 72 hours.

Standard Systems and Applications (SS)
During an emergency, operations and data should be restored within 96 hours.

Emergency Access Procedures for Critical Systems and Data
During an emergency, priority will be given to restoring and supporting operations in the following departments:
1. 911 Center
2. Bradford County Manor
3. CYS, Mental Health, Mental Retardation
4. Prison
5. Accounting

Restoration of Operations for Critical Systems
IT will maintain a database of all applications in use by Bradford County employees and rate the applications according to the priority of restoration that will be required in the case of a disaster or interruption of operations.

Maintenance Window
IT requires a maintenance window on all equipment that it maintains. The maintenance window will be in keeping with the system uptime standards enumerated above. Routine maintenance will be announced and coordinated with the affected department(s).

Table of Bradford County Systems and their Classifications
Type of System
System or Application
Safety Critical Systems (SCS)
1. 911 Center Telephone Systems and Radio System
2. Manor Computer Systems
Mission Critical Systems (MCS)
Vax 3800 Minicomputers, Accounting and Financial Systems, Core Network Equipment
Core Systems (CS)

Standard Systems
County File Servers

Password Policy for Critical/Core Systems
Administrator and Root level passwords and usernames for critical/core systems will be documented and securely stored where they are available only to authorized personnel.

Workstation Security
No network devices, including but not limited to computers, hubs, switches and routers, and wireless devices may be attached to the Bradford County network unless they have been approved in writing by the IT department. Moreover, only members of the IT department or approved contractors may attach network devices to the Bradford County Network. Users may not bring workstations from home and attach them to the network unless approved in writing by the IT department.

All workstations must have county-approved virus protection software on them, configured in accordance with the current Malicious Software Policy.

Workstations will be stored in controlled access areas, or in areas where there is minimal probability of unauthorized personnel viewing screens or data. When workstations must be stored in public areas, screens will be turned away from public view. When this precaution is not possible, covers will be installed in order to preclude passerby access to High Risk and Confidential information.

User Privileges
User privileges on a workstation will be assigned at the lowest level possible. Initially, the user’s workgroup will be assigned User access. However, some applications will not work properly unless the

4/7/2008 Page 178 of 296
user has a higher level of privileges. If this has been demonstrated to be the case, the user will be granted the lowest level required for applications to work properly. Because of the need to push software updates to workstations, the Firewall feature in Windows XP and higher operating systems will be turned off. Workstations will be configured to allow Remote Desktop access to the workstation and will be configured so that appropriate support personnel can login in order to provide technical support.

Screen Savers

Screen Savers will be configured to activate after 5 minutes of inactivity so that High Risk and Confidential information is not visible during periods of user inactivity. Only screen savers and wallpaper backgrounds that come with the Windows operating system are to be used. “My Pictures Slide Show” is not to be used as a screen saver.

Login Banners

When logging in to a workstation or any other Information Systems device in Bradford County, the device will display a logon banner reminding users of their responsibilities to be familiar with County Information Security Policies and of their responsibility to help maintain the security of Bradford County’s information assets.

Backup, Restore, and Media Management

Data Backup and Restore Policy

End users are responsible for ensuring that all County data is stored on county file servers. The IT Department is responsible for backing up and restoring data on servers and is responsible for ensuring the confidentiality, integrity, and availability of the County data that is stored on servers.

IT may delegate the task of changing tapes to other departments whose servers are not in the IT server farm. However, IT is responsible for ensuring the integrity of the tapes and backups. End users who require restoration of data will inform their supervisor and the IT department immediately. They will provide IT with as much information about the data, including the location and the approximate date and time of deletion. Depending on the circumstances, the data may or may not be available for restoration.

a. All servers’ data files will be fully backed up at least once a week.
b. All servers will be incrementally backed up every business day. However, daily full backups are preferred.
c. At least two sets of full backups will be maintained off-site and rotated weekly.
d. An IT staff member will review all server backup logs daily and will record the status of backups on a daily checklist.
e. At least once a month, a member of the IT staff will perform a random test restoration of data from tape in order to ensure the integrity of the backups. The rotation schedule will be such that tapes from each server are tested at least once a quarter.
f. For automated backups, a backup user will be created. Backups will not be performed under the Administrator account.

Archival Backup and Storage Policy

g. All servers will receive annual archival backups and the tapes will be maintained in a safe, offsite location for at least one year.

Media Management Policy and Procedures

Users are not permitted to remove county data from any county premises without express written permission. Removal of backup media for storage at alternate buildings is exempt from this policy. Media containing County Information Assets, including but not limited to floppy disks, CDs, hard disks, and other removable media will be treated in accordance with applicable state and federal statute or regulation. When media is no longer required, it will be turned over to IT for proper disposal. IT will repartition and format all media that is to be redistributed. Media not intended for redistribution will be formatted before being discarded according to applicable regulations.

With federal and state regulations on information security, use of rewritable media including but not limited to diskettes, DVDs and CDs is not authorized without written justification.

If a department has determined a valid need for the use of rewritable media and the media is coming from a source outside the County network, the media must be scanned for viruses prior to using any information on the media.

Maintaining and Monitoring Physical and System Security

Monitoring Information Assets
Bradford County will maintain a record of all activities related to computer hardware, software and network infrastructure equipment, wiring and maintenance. All maintenance requests, adds, moves and changes of these assets will be recorded and documented.

Facility Security Policy
Access to every office, computer room, and work area containing sensitive information must be physically restricted. When offices are not in use, doors must be locked.
Guards, receptionists or other staff must control visitors or other third party access to Bradford County offices, computer facilities, and other work areas containing sensitive information.
Visitors and other third parties must not be permitted to use employee entrances or other uncontrolled pathways leading to or through areas containing sensitive information.

Network Monitoring and Intrusion Detection Policy
All servers and workstations will be configured to monitor activity in accordance with current best practices in information security. At a minimum, login and logout information, and account management information will be monitored and stored in a local machine log or on a syslog server. IT will review the logs on a daily basis for anomalous or suspicious activity. IT will maintain a running daily log verifying that the daily review was performed as well as noting the name of the individual, date, and time that the log was checked.
Application level monitoring will be enabled, when available, for all applications that contain high risk, confidential, or protected information. The supervisor of the department responsible for the application will review the application level logs on a weekly basis for anomalous or suspicious activity. The supervisor will maintain a running log verifying that the review was performed as well as noting the name of the individual, date, and time that the log was checked.
Logs containing security relevant events must be retained for at least three months. During this period, such logs must be secured such that they cannot be modified, and such that only authorized persons can read them. These logs are important for error correction, forensic auditing, security breach investigations, and related efforts.

Time Synchronization
All network devices attached to the Bradford County network will have their internal clocks synchronized with a single time source, maintained by IT.

Incident Response Policy
Users will report all suspicious activities, social engineering attempts, abnormal behavior of equipment, systems or persons, virus activity, and any unusual occurrences to their department supervisor immediately. The department supervisor will report this information to the IT department or the County Security Officer depending on the nature of the incident. The Security Officer and the IT department will conduct an investigation as required by the nature of the incident and will document their findings and report back to the department supervisor within an appropriate amount of time. IT and the security Officer will contact law enforcement agencies if their investigation warrants it.

Procedures for response to a suspected security incident or breach include:
1. Assign and delegate responsibility for managing the investigation into the incident.
2. Gather all evidence related to the incident.
3. Secure any equipment involved in the incident.
4. Secure the facility, if necessary.
5. Contact legal authorities where necessary.
6. Identify new security features to be implemented or modified.
7. Document all information related to the incident.

Virus or Malicious Software
IT will consult virus logs and appropriate security resources and make sure the virus is contained and will try to discover and document the manner in which the malicious software entered the system.

Network Intrusion
Should a network intrusion be suspected, IT will take the following steps:
1. Record and Capture any necessary system information.
2. Backup, isolate, and shut down (if necessary) the compromised system.
3. Search other systems for signs of intrusion.
5. Identify how the intruder gained access.
6. Identify what the intruder did.
7. Collect and preserve evidence.
8. Contact Law Enforcement (if necessary)
9. Identify and implement new security features or procedures to protect from a recurrence of a similar intrusion.

Malicious Software Prevention
Virus screening software must be installed and enabled on all Bradford County servers, workstations, notebooks and all other vulnerable network devices. Virus prevention software will be configured by a member of the IT staff and will be configured for central management (where available) and updating by a central anti-virus server.

Every computer file received from any outside source, including but not limited to diskettes, CDs, DVDs and USB drives from outside the organization, downloaded computer files from bulletin board systems or attachments to electronic-mail (e-mail) messages must, without exception, be scanned for computer viruses by individual department staff or the IT Department.

Patch Management Policy
All systems will be patched in accordance with industry best practices and publisher recommendations. At a minimum, all systems will be patched with the most recent patches at least once a quarter. Firewalls, web servers, FTP servers, and other edge and border devices will be evaluated for patching on a quarterly basis.

IT will monitor industry security resources and respond appropriately to new and ongoing threats. When necessary, IT will take proactive steps to protect County information systems and assets from new and emerging threats.

System Administrative Policies
User Registration Policy
All users of Bradford County Information Systems will be uniquely identified with a unique username and password. Users will not share their passwords with anyone under any circumstances.
Department Supervisors are responsible for contacting IT whenever they have a new or transferred employee who requires access to the network. If IT not notified in writing, IT will write up a request. IT will retain a record of these activities and will maintain an information base of all end-user access to network resources.

IT will create an account with appropriate privileges as requested by the department supervisor and will set a temporary password for the user to enter for the initial login, after which the user will be required to change the password.

End User Passwords
When a user account is created on the network, users are assigned a temporary password that must be changed the first time they logon to the network. After changing this temporary password, Bradford County employees will not divulge their passwords to anyone for any reason! Supervisors and members of the IT staff will never need this information. Should a user account become locked out for any reason, employees will contact IT in order to have the account unlocked.

Password should be obscure and must be a minimum of six characters in length. For best security, passwords will include both uppercase and lowercase and special characters (e.g. "@", "!", ";", "%"). Password must include at least one number. Passwords must be changed no less than every 180 days.

Information Technology Purchasing Policy
Bradford County will use computers in applications where substantial benefits can be realized in increased productivity, better access to information, improved customer service, or lower overhead cost of delivering products and services.

The responsibility for hardware and software purchases represents cooperative and coordinated effort between the Users, IT, and Commissioners.

Only authorized hardware and software will be purchased and installed on the County's computers. No games software is authorized software under County policy unless pre-approved by the Commissioners.
Public domain software must be authorized by IT on an individual basis.
Hardware will be considered for use by the County if it meets standardization requirements and has a proven record for reliability and quality. The selection process for general purpose software will emphasize compatibility and ability to maintain upgraded versions.

The purchase of each individual computer and related software must be fully justified to the Commissioners on the basis of the above criteria.
Cost of purchases must be included in Department’s budget.

Non-County Employee Agreements

All contractors and other business associates of Bradford County will sign an Agreement before they are granted clearance to use any County computer equipment or County network. The exclusion to this would be computers setup to be accessed by the public.

Workforce Clearance Policy

All workers to be placed in sensitive positions that will have access to High Risk or Confidential County Information Assets must first pass a background check in accordance with applicable state or federal statute or with County and departmental procedures.

IT

Individuals hired by the IT department may have access to all county information assets in every department. Therefore a background investigation in accordance with the strictest applicable policy will be performed. Persons who have been convicted of a felony must not be hired into, retained for, promoted into, or maintained in computer-related positions of trust.

Employee Termination Policy

When an employee with computer access is to be terminated for cause, HR will notify IT in advance. If advance notice is not possible, IT will be notified as soon as possible afterward so that appropriate measures can be taken to protect County Information Assets and forensic evidence, if required.

IT will immediately revoke the employee’s access to all systems to which they have access and secure their data so that it will be available for future legal or management review, if required.

When an employee leaves County employment, regardless of reason, a checklist will be used by HR and the departmental manager to ensure that all County property, including but not limited to keys, computers, PDAs, and files have been returned.

Contingency Operations, Emergency Operations, and Disaster Recovery Operations

Each Bradford County department is required to have in place an Emergency Mode Operations and Disaster Recovery Plan that, at a minimum, addresses the following issues:

1. How the department will conduct business during an emergency.
2. Define the key resources that are required for emergency operations and enumerate how those resources will be provided.
3. The backup location(s) where the department will conduct operations.
4. How the department will contact key personnel in an emergency.
5. How the department will disseminate information during an emergency.
6. Enumerate a timeline for the reconstruction of normal operations
7. Each department is required to test and revise the Emergency Operations Plan annually.

Departments will review and test their plans annually for accuracy and relevance and maintain a copy on file with the Bradford County Commissioners.

Exception Clause

The IT Department reserves the right to make exceptions to any part of this policy when the need arises. Only the IT Department Head can give approval for any written requests from the Department Head(s) for deviations from the policy. Any County employee found in violation of this policy without written permission from the IT Department will be subject to disciplinary action up to and including termination.
Policies and Procedures for the Acceptable Use of Computers and Technology

Purpose
To provide clear guidelines to all employees and Elected Officials regarding access to and disclosure of computer and network systems, including electronic communications involving electronic-mail (e-mail), Internet and downloading of computer files which are sent or received by County employees with the use of any County computer communications systems. Also, to ensure the safety of the investment Bradford County has made in computer hardware, software, training, and labor.

Background
Data processing information has become a vital resource of the County and is critical to the day-to-day operation of the County. This information, like any other asset, must be protected.
As Personal Computers and Local Area Networks are used increasingly in County employees’ daily activities, it becomes increasingly important that these tools be used properly and efficiently.
The computer should be employed where results are measurable in terms of efficiency, improved quality of work, increased productivity and/or improved service to the customer. Computers may also be deployed as an aid in training.

Scope
The variety of computing and electronic communication access and tools that the County provides its employees include but are not limited to desktop, laptop, mobile and central computers, internal and external networks, electronic mail (e-mail), Internet, modems, and facsimile systems. These tools are County owned and publicly funded; the computer systems and the software information contained on or conveyed through them are the property of the County. Access and use are restricted by these Computer Policies and Procedures. Equipment that is the property of another entity, but used by County employees in the course of their work, is also encompassed in this policy. Telecommunications and Commonwealth of Pennsylvania computer systems and networks are not included in this policy.

By addressing the issues of use for computer communications, the County ensures maximum benefits by recognizing a critical and defined balance between the need for open communications and the protection of County assets. Each system may, at times, have its own set of policies and procedures. In those cases where communications are carried across other regional networks or the Internet, employees of the County are advised that the most restrictive and security conscious policies takes precedence over acceptable use policies of those other systems.

Responsibilities
Departmental Management
* Fully justifies to the Commissioners the need for the computer, related equipment, and software before purchasing.
* Purchases must be included in Department’s budget.
* Provides necessary security over equipment, software, and data in accordance with the procedures defined in this manual.
* Responsible for verifying accuracy of reports.
* Develops and maintains software user manual if one is not supplied by vendor or is inadequate to meet the Department’s needs.
* Develops and implements backup procedures in accordance with the County’s policies and procedures.
* Verifies and signs off on the accuracy of reports and modifications made to the department’s application software.
* Allocates sufficient time for employees utilizing computers and software to learn the application and become productive users.
* Cross trains employees on the operation of critical applications.
* Monitors activities with respect to computers to ensure compliance with policies and procedures set forth by management.
* Responsible for annually reviewing the listing provided by IT of hardware and software allocated to their department to determine the list’s accuracy and notifying IT of any discrepancies.
* Maintains the security and confidentiality of sensitive information.
* Must ensure that each computer user in their department has received in-service training on security and read and signed the “Employee Agreement for Computer Usage” before that employee is allowed access to a computer and/or network systems. The signed agreement will be kept in the employee’s personnel file.

* All users of Bradford County Information Systems will be uniquely identified with a unique username and password. Users will not share their passwords with anyone under any circumstances.

* Department Supervisors are responsible for contacting IT whenever they have a new or transferred employee who requires access to the network. If IT not notified in writing, IT will write up a request. IT will retain a record of these activities and will maintain an information database of all end-user access to network resources.

* All workstations must have county-approved virus protection software on them, configured in accordance with the current Malicious Software Policy.

* Workstations will be stored in controlled access areas, or in areas where there is minimal probability of unauthorized personnel viewing screens or data. When workstations must be stored in public areas, screens will be turned away from public view. When this precaution is not possible, covers will be installed in order to preclude passerby access to High Risk and Confidential information.

User

* End users are responsible for ensuring that all County data is stored on county file servers. The IT Department is responsible for backing up and restoring data on servers and is responsible for ensuring the confidentiality, integrity, and availability of the County data that is stored on servers.

* When a user account is created on the network, users are assigned a temporary password that must be changed the first time they logon to the network. After changing this temporary password, Bradford County employees will not divulge their passwords to anyone for any reason! Should a user account become locked out for any reason, employees will contact IT in order to have the account unlocked.

* No devices including but not limited to PDAs, USB drives, cameras and phones shall be connected to a computer without IT authorization.

* No network devices, including but not limited to computers, notebooks, hubs, switches and routers, and wireless devices may be attached to the Bradford County network unless they have been approved in writing by the IT Department. Moreover, only members of the IT department or approved contractors may attach network devices to the Bradford County Network.

* Properly uses equipment, Internet and E-mail.

* Understands confidential nature of stored information and maintains its security.

* If notebook is taken offsite and documents are stored on it, documents must be immediately uploaded to server as soon as return to office.

* Users are not permitted to remove county data from any county premises without express written permission. Removal of backup media for storage at alternate buildings is exempt from this policy.

* Users will report all suspicious activities, social engineering attempts (see Section 2 for more detail), abnormal behavior of equipment, systems or persons, virus activity, and any unusual occurrences to their department supervisor immediately. The department supervisor will report this information to the IT Department or the County Security Officer depending on the nature of the incident. In the event that reporting a violation to an immediate supervisor is in appropriate or uncomfortable, the report should be made directly to the IT Department or Personnel Director.

* Once a week, IT downloads at night operating system upgrades and new virus definitions to computers connected to the network. The user must have the computer turned on but logged off on this designated night of the week. Contact IT to find out which night this is.

Expectation of Privacy

Users should have no expectation of privacy when using information systems at Bradford County. To manage systems and enforce security Bradford County may log, review, and otherwise utilize any information stored on or passing through its systems. For these same purposes, Bradford County may also capture User Activity such as telephone numbers dialed and web sites visited.

Copyright Policy

Bradford County will comply with the copyrights and software licenses for all software that it purchases. Bradford County employees will not install or run or permit anyone to install or run copyrighted software on Bradford County computers unless the County is so authorized under a software license. Furthermore, Bradford County employees will not copy licensed software or permit it to be copied in violation of the County’s software license.
In most cases, software purchased by departments for use on computers will include a Software License Agreement. By opening the sealed software package, a user has shown agreement to the license terms put forth by the software producer.

All users should read, fully understand, and comply with the licensing agreement that is included with each software package the County purchases. The following terms are typical of those found in most licensing agreements, and should serve as general guidelines for users:

1. **COPYING**: You agree not to copy the software for the purpose of providing another user with a copy of that software. Copying for the purpose of providing yourself with a backup should your original diskette or CD get damaged, is, however, allowed.

2. **LIMITED USE**: You agree only to use the software on a single or subsequent (but not additional) personal computer. You agree not to use the software on two computers at the same time unless purchased under a multi-user license agreement. You agree not to, without prior written consent, rent, lease, or lend the software to another party.

Most software contains proprietary information and is protected by federal copyright laws. Damage awards for software copyright violations may be awarded on each illegal copy for each day the software was illegally installed. All users should be fully aware of the terms of software license agreements and the consequences of violating these terms.

Situations involving violation of this policy may be cause for disciplinary action and could lead to termination of employment.

**Use of County Purchased Hardware and Software**

Employees will not remove any hardware or software from their work locations without the expressed prior consent of their supervisors. Failure to comply with this policy will be construed as employee theft and become grounds for dismissal or other disciplinary action.

If a supervisor finds it necessary for an employee to remove computer hardware or software (including making copies of computer programs), from their work locations, they must notify IT IN WRITING prior to such removal. The written permission will be maintained for one year. The written permission must include:

1. Dates covered by removal
2. Whether daily removal will be required by employee
3. That the employee is responsible, within reason, for the equipment and information being removed
4. That only authorized employees will be using the equipment
5. That the employee agrees to immediately upload the information to the server upon return to the office.
6. The employee and department head must sign release with the above information.

This policy DOES NOT include removing off site tape or disk backups of data created and used solely for disaster recovery purposes.

**Use of Non-county Software on County Equipment**

No software may be loaded or run on County computers UNLESS:

1. The County has purchased and received the software from an authorized dealer.
2. IT has authorized the software’s use and scanned it for any viruses.

Instant Messaging software is not to be used on County Equipment.

Failure to comply with this policy will become grounds for dismissal or other disciplinary action. For purposes of this policy, software is defined as any program or operating system.

**Use of Non-county Equipment**

Users may not bring equipment from home and attach it to the network unless approved in writing by the IT department.

No personal electronic equipment, including but not limited to notebooks, PDAs, Ipods, phones, cameras, USB drives and CD/DVD drives may be used with Bradford County equipment unless they have been approved in writing by the IT Department.

County documents and files are not to be accessed by County employees from Non-County equipment without written permission from IT. This is to protect the County network from viruses and to help insure confidentiality of information.

**Non-county Employees**

Non-county Employees accessing the Bradford County network or computers will be asked to sign a Non-County Employee Computer Usage Agreement. It will be the Department Head’s responsibility to get an agreement signed. No agreement is needed for non-county employees who are using computers setup for public access.
Working From Home
Working from home must be pre-approved by the Commissioners. There must be written justification and will be decided on a per case basis.

Screen Savers and Wallpaper
Screen Savers will be configured to activate after 5 minutes of inactivity so that High Risk and Confidential information is not visible during periods of user inactivity. Only screen savers and wallpaper backgrounds that come with the Windows operating system are to be used. “My Pictures Slide Show” is not to be used as a screen saver.

Section 2 – Information Security

Security
The confidentiality, integrity, and availability of county information and information systems are of the utmost importance to the daily operations of Bradford County. It is the responsibility of every user of county information assets (including both electronic systems and documents) to help maintain the security of the information.

Any information that due to legislative mandate or other cause is defined as sensitive or confidential in nature must be kept secure. Confidential information includes any information protected by County, State or Federal privacy acts or administrative regulations. In addition, it should include anything that in the opinion of the department head would be appropriately kept confidential in order to protect the interests of the County, its employees, or its clients, so long as such action by the department head does not conflict with relevant open meetings and records statutes.

The level of security provided should be that required by statutory mandates or that which is appropriate to the sensitivity of the information. Each department head shall be responsible for developing and maintaining the appropriate security procedures necessary to ensure compliance with confidentiality requirements.

Due to confidentiality of information, e-mails will only be accessed through connection with the Bradford County network.

Types of security may include:
1) Key locks on personal computers
2) Key locks on file cabinets, drawers and other locations where documents are stored
3) Limited facilities access, such as locking an office door.
4) Software access security to local hard disks or directories.
5) Local Area Networks ID, Password, and Directory security.
6) Logging off the network when away from workstations for lunches or breaks.

Due to sensitivity of information and locking of data, users are to exit applications prior to leaving their workstations. If leaving for longer than fifteen minutes, user must logoff from network. Where logging off is not a viable option, user must lock their computer

Social Engineering
Beware of attempts that ask you to divulge information about the network, your network password, your username, and other information related to the systems in use at Bradford County.

The easiest way for criminals to gain access to networks is for them to simply ask an unsuspecting user for their user name and password while posing as a technical support person. No member of the Bradford County IT staff or any contractor will ever ask for your username and password. Never divulge this information to anyone! Should a member of the IT staff need to access your account, they will change your password and reset it after they have finished their work. If anyone does ask for this information, the event should be reported to the IT staff immediately.

Another common method for obtaining information is through the use of Phishing. County staff, banks, state agencies and companies such as Microsoft will never send you an e-mail asking you to confirm login information. Should you get an e-mail from an organization asking you to login and confirm some information, do no use the link in the e-mail. Rather, go directly to the home page of the organization or call on the phone to see if this is a valid request.

Virus and Malicious Software Policy
Every computer file received from any outside source, including diskettes from outside the organization, downloaded computer files from bulletin board systems or attachments to electronic-mail (e-mail) messages must, without exception, be scanned for computer viruses by individual department staff or the IT Department.
The County, and its individual department heads or supervisors, reserve the right to access, inspect, review, and/or monitor computers and network communications systems at any time. By using the County’s computers, or networks, the employee is voluntarily consenting to being monitored. Managers and supervisors may inspect the computers or review the computer communication systems of the employees they supervise to determine whether there have been any breaches of security, violations of County policies, or other violations of duty on the part of the employee(s). The County, and its individual department heads or supervisors, at its discretion, may also use computer programs that monitor computers, networks, Internet or computer communications systems for purposes of assuring system security and compliance with County policies. The Local Area Network security must be utilized by each department that has a local Area Network installed.

Data Security Policy
County Information Assets will be handled in accordance with their Data Classification and in accordance with appropriate federal and state statutes and regulations. Bradford County employees may be in a position to receive confidential information during the performance of their duties. County employees shall never use information obtained confidentially for any purpose and shall respect the privacy of individuals. Since public access of information varies, employees should consult with their supervisor/department head regarding the dissemination of privileged information. Violations of this confidentiality requirement will be grounds for disciplinary action, including dismissal.

Document Security

Network Printing
When users are printing High Risk and Confidential data they will take precautions to ensure that their privacy and security are protected. Examples of this include
1. Standing by the printer while the job is printing.
2. Immediately remove the documents from the printer.
3. Print to a printer/copier mailbox and release the print job when standing at the printer/copier.

File Cabinets and Record Rooms
1. File cabinets that contain High Risk and Confidential Data will be kept locked at all times.
2. File Rooms will remain locked when unattended.

Data Transmission & Encryption Policy
High risk data must be encrypted during transmission over insecure channels. An insecure channel is defined as any public network, including but not limited to the Internet. Confidential data should be encrypted during transmission over insecure channels. Bradford County Employees are not permitted to encrypt or apply passwords to data unless it is for the purpose of transmission over an insecure channel.

Password Policy
Bradford County employees with computer or network access are required to have one or more passwords in order to login and authenticate to the network or to applications that are required in the performance of their official duties. The County, and its individual department heads or supervisors, reserve the right to override passwords and codes at any time.

Network Passwords
When a user account is created on the network, users are assigned a temporary password that must be changed the first time they logon to the network. After changing this temporary password, Bradford County employees will not divulge their passwords to anyone for any reason! Supervisors and members of the IT staff will never need this information. Should a user account become locked out for any reason, employees will contact IT in order to have the account unlocked.

Application Passwords
Many employees also require application-level passwords. In most cases, the procedure will be handled in the same way as Network Passwords are. However, in rare cases, the password will have to be assigned by an application administrator and may not be able to be changed by the employee. Only department heads are to have a list of these passwords, if necessary. This list must be kept in a secured location.

Document Level Passwords
Passwords will not be used on documents, including but not limited to word processing documents, spreadsheets or any other data belonging to Bradford County. Passwords are allowed to be used on spreadsheets to protect formulas but not data.

Guidelines for Passwords

The best practice for password management is to refrain from writing down passwords. However, Bradford County recognizes that some users may have to remember many passwords for different systems. If the user must write down passwords, the following guidelines must be followed:

Users will be held responsible for the unauthorized use of his/her password by another person.
Password should be obscure and must be a minimum of six characters in length. For best security, passwords will include both uppercase and lowercase and special characters (e.g. “@”, “!”, “&”, “%”). Password must include at least one number.
Do not use family member names, pet names, birth dates or any other information that would be easily guessed about you.
Change password when:
1) Unauthorized person learns password
2) Authorized person who knows password leaves employ of Bradford County or transfers to a position where no longer authorized to know password.
3) Password expires.

Removable Media Use and Retention

Users are not permitted to remove county data from any county premises without express written permission.

With federal and state regulations on information security, use of rewriteable media including but not limited to diskettes, USB drives, DVDs and CDs is not authorized without written justification.
If a department has determined a valid need for the use of rewriteable media and the media is coming from a source outside the County network, the media must be scanned for viruses prior to using any information on the media.

Modem Use

Modems may not be attached to any County computer unless it is authorized in writing by the IT department. Only a member of the IT department is authorized to install and configure a modem that will be attached to a computer that is on the Bradford County Network.
Modems leave a network open to security breaches.
Modems will not be left connected to personal computers in autoanswer mode, such that they are able to receive incoming dial-up calls.
Remote access to personal computers by dial-up or other means must be approved by the IT department.
All communications in remote access sessions over the Internet or over any other unsecure network must be encrypted with a County approved encryption method.
Users should be made aware of the risks and responsibilities of PC modem use by their department head.
It will be grounds for immediate termination if these procedures are not followed.

Quality Assurance of Business Critical Information

Each individual that produces reports or other information that is used to make business decisions within the County must have a process in place to verify that the information being provided is timely, accurate, and correct.
It is the responsibility of each supervisor to ensure that the employees under their control have developed and are using procedures to ensure the quality of business critical information. These procedures may include: cross footing totals in spreadsheets, reasonableness checks of raw and summary data, having another individual review your spreadsheet formulas or database program, etc.

Maintenance and Repair

In order to function as a productive tool, a computer must be maintained in good working order. It is the responsibility of the User to keep computer equipment in good working order by following proper daily procedures for computer care, performing periodic routine maintenance, and reporting equipment failures for appropriate corrective action. Guidelines for daily care, routine maintenance and troubleshooting problems can usually be found in the manuals provided with the equipment.
When a problem with computer equipment is encountered, the User must follow the proper procedure for reporting the failure and assuring that corrective action is taken.
1) At the time a failure occurs, the User should make every effort to document the failure as much as possible. If an error message appears on the screen, the User should immediately record the message by printing the message to a printer. If there is not a printer on the system, the error message should be written down exactly as it appears. The time, date and what user was doing when the error occurred should also be noted.

2) After the failure is properly documented, the User should contact IT for assistance. If the failure is intermittent in nature, the User may be requested to continue operation of the system until failure becomes consistent enough to correct. If the failure is constant and is preventing productive use of the system, IT will take corrective action.

3) IT will take prompt corrective action to see that down-time due to computer equipment failure is minimized. Corrective action will consist of initiating a service call to the outside service agency responsible for computer repair.

4) In instances where the use of the computer is critical to the operation of the County, IT will make reasonable effort to minimize work interruption due to equipment failure by attempting to provide or procure loaner equipment for the user.

5) It is the responsibility of the User Department to perform preventative maintenance on equipment within the department. Check the manuals that came with the equipment.

Section 3 – Electronic Mail (E-Mail) and the Internet

Policy Statement

E-mail is considered by the County to be an important form of County communication. All communications within our intra-county computer network and sent or received through the Internet, including the contents of an employee’s computer, are the property of the County. All communications should be professional in nature. The use of these systems for defamatory, obscene, sexually explicit, illegal, offensive, threatening or other inappropriate communications is strictly prohibited.

If you become aware of someone using computer resources for any of these activities, you are obligated to report the incident immediately to your supervisor. In the event that reporting a violation to an immediate supervisor is inappropriate or uncomfortable, the report should be made directly to the County Personnel Director.

Improper use of the County’s computer resources or network is grounds for discipline up to and including discharge.

Use of computer resources for any of these activities is strictly prohibited:

* Disseminating or storing commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political information, religious information or any other unauthorized material.

* Wasting computer resources by, among other things, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, engaging in non-work related online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.

* Employees may not use the County’s Internet connection to download games or other entertainment software, including screen savers, to play games on the internet or to gamble.

* Using or copying software in violation of a license agreement or copyright

* Violating any state, federal, or international law.

* The County’s computer communication systems are for the use of persons legitimately affiliated with the County.

* Receiving streaming video or audio that is not for official purposes.

* Using instant messaging

* Accessing information through email or Internet that would violate the County’s Sexual Harassment Policy, or that is of a sexual or pornographic nature.

Personal Use of Computers, Networks, Internet or Electronic Mail

Limited, appropriate personal use of the computer system is permitted during lunch hours, break times and before or after work hours when the use does not (1) interfere with the user’s work performance; (2) interfere with any other user’s work performance; (3) have undue impact on the operation of the computer system; or (4) violate any other provision of this policy or any other policy, guideline, or standard of Bradford County. At all times, users have the responsibility to use computer resources in a professional, ethical, and lawful manner. Personal use of the computer system is a privilege that may be revoked at any time.

Monitoring and Control
The county retains the right to monitor all Internet usage and E-mail messages during the ordinary course of its business without notice to the user, sender or recipient of the message, except as restricted by applicable law. For example, monitoring may be necessary to protect and ensure the system’s security, to ensure that employees are not using e-mail to communicate improper content, such as unlawful harassment, improper management techniques, unauthorized disclosure of confidential information and trade secrets, and to ensure that employees are not communicating to unauthorized recipients. The County may actively monitor Internet usage and E-mail communications, and reserve the right to inspect any and all files stored in private areas of our computer systems in order to ensure compliance with the policy. The County reserves and will exercise the right to review, audit, intercept, and disclose any matter on the system at any time to the fullest extent of the law.

Expectation

Since all E-mail messages are the property of the County, we may monitor these communications to ensure that our system is being used for legitimate business purposes only, and to protect the County from Liability. Employees and those communicating with employees must realize that they have no right or expectation of privacy in their E-mail communications. All messages are subject to review by management, and all communications are subject to scrutiny, except as restricted by applicable law. The use of an employee provided password does not affect the County’s ability to access messages.

Warning: All messages sent using electronic mail have the potential to be viewed by anyone, therefore, employees should not have an expectation of privacy in anything they create, store, send or receive on the computer system.

Permanency of Communications

Deleting E-mail messages does not guarantee that they are erased from the system. Employees should not believe that privacy of E-mail communications is created by their efforts to delete incoming or outgoing messages. In addition, in the case of litigation, technology may exist to restore deleted E-mail. Employees should be prepared to defend in court under oath the content of anything communicated in an E-mail. Employees should not comment on issues that are in litigation or are capable of turning into litigation.

No Harassment

No E-mail messages should be created or sent which might constitute intimidating, hostile or offensive material on the basis of sex, race, color, religion, national origin, age, sexual preference or handicap or disability. Harassment is broadly defined as anything which has improper (e.g. sexual) content and is both unwelcome and offensive to a reasonable person. The display of any kind of sexually explicit image or document in any County system is prohibited. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using County network or computer resources. Please refer to the County’s policy against sexual harassment.

Ultimate responsibility for any directly or indirectly connected traffic that does or does not conform to this policy is with the individual employee who originates or accesses that traffic. The County accepts no responsibility for traffic which an employee originates which Violates this policy.

The following footer should be appended to all confidential e-mail sent outside of the County network:

This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by the attorney-client privilege. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify _______________ by telephone at __________. You will be reimbursed for reasonable costs incurred in notifying us.

Internet Usage

The same policies applied to e-mail use also apply to the use of the Internet. Employees are not permitted, without prior authorization, to establish web pages which suggest County affiliation or other authorization by the County. Employees may access and use the Internet through the County’s system, computers, modems or lines only for specifically approved purposes. Any software or files downloaded via the Internet into the County network become the property of the County. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. No employee may use County computer resources knowingly to download or distribute pirated software or data. The County’s Internet facilities and computer resources may not be used knowingly to violate in any material way the laws and regulations of the United States or any other nation, or the laws or regulations of any state, city,
providence or jurisdiction. All communications on the Internet to or from the County's system or computers owned or operated by the County are subject to monitoring except as prohibited by law, and to all of the County's standard policies. All communications should be professional in nature. Bradford County is not responsible for material viewed or downloaded by users from the internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

If an inappropriate site on the internet is accessed accidentally, the user should:
1) Make note of the date and time the site was accessed.
2) Make note of the website accessed.
3) Contact IT with this information, so a log can be made of the accident.

Persons needing in the course of county business to originate traffic or access sites which a reasonable person might find offensive, must notify their department head in writing of their intent to access and/or originate such traffic (e.g. A law enforcement officer or social worker may need to originate or access traffic on sexual predators). This written documentation will be maintained for one year.

Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, subscribing to non-business-related list-servers and mailing lists, spending excessive amounts of time on the Internet, playing games, engaging in non-work related online chat groups, instant messaging, listening to audio, watching video (including weather), printing multiple copies of documents, or otherwise creating unnecessary network traffic.

If an inappropriate site on the internet is accessed accidentally, the user should:
1) Make note of the date and time the site was accessed.
2) Make note of the website accessed.
3) Contact IT with this information, so a log can be made of the accident.

Persons needing in the course of county business to originate traffic or access sites which a reasonable person might find offensive, must notify their department head in writing of their intent to access and/or originate such traffic (e.g. A law enforcement officer or social worker may need to originate or access traffic on sexual predators). This written documentation will be maintained for one year.

Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, subscribing to non-business-related list-servers and mailing lists, spending excessive amounts of time on the Internet, playing games, engaging in non-work related online chat groups, instant messaging, listening to audio, watching video (including weather), printing multiple copies of documents, or otherwise creating unnecessary network traffic.

It is recommended when sending attachments; always identify the attachment by the application and version used to create it. For example “The attached WordPerfect 6.0 document...is saved to ASCII.

Limit the size of the messages that you send.
As a courtesy to the recipient of a “reply” message, include the original message (if the size of the original message makes this practical).
Limit the number of people on your distribution lists (routing slips) to those who really need the information. This helps avoid information overload for those who do not need the information.
Use clear and concise subject headings to give your recipient an advanced indication of the message contents.
Limit the use of “high priority” mail. Overuse may dilute the true urgency of any future mail.
There are additional methods of communication for urgent messages. Your recipients may not check their e-mail messages as frequently as you do. If it is imperative that you contact someone immediately, consider phoning or paging them.
Delete messages you no longer need. This includes your Out Box and Trash, as well as your In Box.
Check your e-mail regularly. At least three (3) times per day is a good reference.
Retention
Retention schedules, based on content of messages, are the same regardless of the medium, paper, voice, or electronic.
E-mail messages and attachments that meet the definition of records shall be disposed of in accordance with applicable law and records retention and disposition schedules approved by the County. E-mail messages and attachments that do not meet the definition of records should be deleted immediately.
E-mail messages, in and of themselves, are not a single record series. Retention and disposition of e-mail messages depends on the function and content of the individual message.
Due to the finite space available for storage, messages should not be kept for longer than one month. Records must be deleted from an e-mail system if their required retention period has expired or after they have been copied to a record-keeping system. Records may be maintained on a manual or electronic record-keeping system. Records shall include transmission or receipt data.
When duplicate copies of e-mail messages are sent internally, the sender will be responsible for maintaining the primary copy for the full applicable retention period. All other copies should be disposed of in accordance with approved records retention schedules relating to transitory messages.
Departments shall establish standards/procedures to manage the storage of records on e-mail and shall not rely on e-mail server backup procedures to manage the retention and disposition of records created in e-mail systems.

Exception Clause

The IT Department reserves the right to make exceptions to any part of this policy when the need arises. Only the IT Department Head can give approval for any written requests from the Department Head(s) for deviations from the policy. Any County employee found in violation of this policy without written permission from the IT Department will be subject to disciplinary action up to and including termination.
Purpose
To establish an individual within each department who would be the responsible liaison for that
department's computer activities. The role of the computer representative is to support the effective and
efficient use of computer systems within his or her department. This person acts as the conduit for all
requests pertaining to the department's computer systems and as the first line of defense in resolving
computer related problems or issues.
Guidelines and Procedures
The computer representative will have a general working knowledge of his or her department's computer
systems. Each representative will be selected by his or her department head through consultation with
the Director of Information Technology and is responsible for:
A. Assisting Information Technology with system security, menus and password assignments. All systems
containing vital or valuable information must be protected against theft or destruction by a password
system.
B. Requesting routine installation of software programs. This includes software not supported in general
by the Village, but specific to the department. If the application is supported by an outside vendor then the
representative is responsible for notifying Information Technology about the vendor and the application.
C. Assisting in basic computer problem resolution. If local problem resolution is not obtainable, the
Information Technology Department should be contacted for additional help.
D. Distributing Village communications regarding current and future microcomputer/automation projects
and training.
E. Attend monthly User Group meetings.
F. Providing Information Technology with vendor hardware service repair information following service
calls, if necessary.
G. Notifying Information Technology of departmental hardware, software application needs, computer-
related problem areas, and training needs.
071 Livonia, MI – Internet Access and Electronic Mail Policy

Internet Access Usage and Electronic Mail

Purpose
To establish the proper use of Internet access and Electronic Mail (E-mail) provided to employees for use in their jobs by the City of Livonia.

Ownership
Internet access and E-mail is provided for the purpose of conducting city business. All electronic communications generated by employees while using this access are the property of the City of Livonia and, therefore, are not considered private. Employees must have their Department Head's approval to request an E-mail address.

Employee Responsibilities
The city imposes certain responsibilities and obligations on employees while using Internet access and E-mail provided by the city. The following serves as a guide for employees when using the Internet:

• Employees are expected to protect their individual user ID and passwords from unauthorized use. User ID's and passwords are not to be shared with any other person.
• Employees should be aware that the Internet is not a secure method for transmitting confidential information. Any message sent across the Internet may potentially be accessed by other individuals. Thus, in some cases, e-mail may not be the proper means of communication.
• Employees are expected to demonstrate the same high standards that apply to other forms of city communications. Please note, that e-mails may be subject to disclosure under the Michigan Freedom of Information Act. Employees are expected to demonstrate courtesy and good judgment in their use of the Internet. Employees are prohibited from sending messages containing offensive, abusive, threatening, or other inappropriate language.
• Employees should be mindful of the record retention requirements under state law.
• Employees are expected to respect the legal protection provided to programs and data by copyright and license.

Monitoring Use
The City retains the right to review and monitor usage of Internet access and E-mail that it provides for the use by its employees. Supervisors are responsible to monitor their employees use of the Internet access.

Violations
Any violation of this policy may subject the employee to disciplinary action, up to and including, discharge from employment. The following employee, by his/her signature, indicates that they have read and understand the above policy and agree to comply.
Personal Information Policy

Purpose: To define basic policies in regards to dealing with Personal Information.

Description:
Personal Information is defined as: first name or first initial plus the last name linked to 1 or more of the following: Social Security Number, Driver License or State Id Number, and/or bank account or credit/debit number along with security code, access code or password. Every effort must be made to keep this information secure. It should not ever be stored on a non-secure media or be sent by e-mail unless encrypted. It should not be removed from City facilities on a CD, DVD, Memory Stick, Laptop Computer, PDA or other device without prior approval by Senior Management.

In the event of a security breach of any source containing this personal information, the City must notify each Michigan resident for whom personal information had been maintained in this source, without reasonable delay as required by the Identity Theft Legislation from 2007.
073 Livonia, MI – User ID Policy

User Id’s
Purpose: To provide consistency in the way User Id’s are defined.
Description:
User Id’s that are set up by the Information Systems Department shall be made up the following information:
First initial of user’s first name
User’s last name
If this combination is not unique, an additional character will be inserted between the first initial and last name. This character may be either a middle initial or another character of the user’s first name. There will not be any duplicate user id’s. If the system does not allow for the entire user’s last name, the user id will be truncated to meet the requirements of that system.
Setting up a Personal Computer
Purpose: To provide consistency in the way personal computers are set up.
Description:
The following steps are to be done when setting up a computer:
1. Install Operating System and Needed Device Drivers
2. Install Network Client (TCP/IP only)
3. Label with Orange ID Label (workstation label)
4. Change Computer Name to match attached standards. (Department code then workstation number)
5. Install needed Application Software.
6. Set the TIA to the correct number in the Environment area.
7. Install Corporate Edition Norton Antivirus
8. Follow up and update Track-it information after the Wednesday Audit.
System Backups
Purpose: To document the rotation and movement of backup tapes and procedures.
Description:
The Information Systems Department backs up three different environments. Each methodology is listed below.
AS/400 The IBM AS/400 is backed up Monday through Friday (with the exception of holidays) on 13 GB ¼” Tapes. Backups are done using the native software included with OS/400. Tapes are maintained on a four-week rotation. The weeks are identified as: 1 – Payroll 1, 2 – Non-Payroll 1, 3 – Payroll 2, 4 – Non-Payroll 2. Every two weeks a set of two weeks is exchanged with a set from the City Hall Annex. Each weeks rotation consists of five (5) tapes labeled Monday-Friday. Every two weeks the Thursday Payroll tape will be taken off-site to DPW and placed in the Fire Resistant Safe. Special backups will be retained for year-end at the request of the Accounting Department. These backups are scheduled to run at 23:00 each night.
Network The Network Servers are backed up Monday through Friday on 50/100 GB AIT Tapes. Backups are done using Arcserve 2000. Tapes are maintained in a Compaq Storageworks SSL 2020 Tape Library Unit. Tapes will be rotated on a three (3) week rotation. Every two weeks, the most recent Friday tape will be taken off-site to DPW and placed in the Fire Resistant Safe. These backups are scheduled to run at 21:00 each night.
Web Server The City’s main web server is backed up on Friday every week on a 35/70 GB DLT Tape. Backups are done using the Backup software included with Windows 2000. Tapes will be rotated on a four (4) week rotation. Every two weeks, the most recent tape will be taken off-site to DPW and placed in the Fire Resistant Safe. These backups are run manually by a Computer Administrator II.
DPS DPS uses eight backup tapes numbered 1 through 8 to backup the server Monday through Friday. Every other week (payday) they take the tape from the server and store it off site in our telephone safe at city hall. The tape from the off site location is put into the number rotation with the remaining tapes in our telephone safe located in the file cabinet next to the server. Tom Mitchell and Brian Wilson both have keys to the safe. By using 8 tapes we don’t attempt overwriting a tape in the saved set. With the use of numbered tapes we don’t have any problems with holidays falling on various days of the week. If a holiday falls on a Friday we take the tape off site on Thursday. Tom Mitchell changes the tapes daily. When he is unavailable, Brian Wilson is his backup. Parks currently uses 5 of their 7 tapes in rotation, Labeled Monday through Friday. The tapes are located in the server closet. Each week, on Friday a tape will be taken off site and stored in the server room at city hall.
Louise Heyza changes the tapes daily. When she is unavailable, Debra Finkbeiner is her backup.
Problem with Backup If there is a problem with a backup, the problem will be logged in Track-It and the Information Systems Director will be notified, in his absence, the Finance Director will be notified.
Virus Protection

Purpose: To document our Virus Protection procedures.

Description:
It is the responsibility of everyone who uses the City of Livonia's computer network to take reasonable measures to protect that network from virus infections.
This policy outlines how various viruses can infect the City of Livonia's network, how the City of Livonia's IS department tries to prevent and/or minimize infections, and how the City of Livonia's network users should respond to a virus if they suspect one has infected the City of Livonia's network.

How viruses can infect the City of Livonia's network
There are actually three various types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. When an infected file is opened from a computer connected to the City of Livonia's network, the virus can spread throughout the network and may do damage. A Trojan horse is an actual program file that, once executed, doesn't spread but can damage the computer on which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

Viruses can enter the City of Livonia's network in a variety of ways:
• E-mail—By far, most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect the City of Livonia's network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.
• Disk, CD, Zip disk, or other media—Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
• Software downloaded from the Internet—Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.
• Instant messaging attachments — Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software.

How the City of Livonia's IS department prevents and/or minimizes virus infections
The City of Livonia's IS department fights viruses in several ways:
Scanning Internet traffic—All Internet traffic coming to and going from our network must pass through company servers and other network devices. Only specific types of network traffic are allowed beyond the organization’s exterior firewalls.
For example, an e-mail message that originates outside of the network must pass through the Norton Anti-Virus for Exchange before it is allowed to enter the e-mail server. This device routes suspicious e-mail and attachments to an isolated storage device, defeating the purpose of a virus.
Running server and workstation antivirus software—All vulnerable servers run Corporate Edition of Norton Anti-Virus. This software scans our file-sharing data stores, looking for suspicious code.
Corporate Edition of Norton Anti-Virus is also installed on all organization workstations. This software scans all data written to or read from a workstation's hard drive. If it finds something suspicious, it isolates the dubious file on the computer and automatically notifies the help desk.
Routinely updating virus definitions — Every hour, the server virus scanning programs check the Symantec Website for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated, and then the system administrator is informed.

When end users turn on their computers at the beginning of the workday, the workstation virus protection program checks with a City of Livonia server on the network for updates. The workstation program will then download and install the update automatically, if one exists.
How to respond to and report a virus

Even though all Internet traffic is scanned for viruses and all files on the company’s servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee’s workstation, and if not properly handled, it could infect the City of Livonia’s network.

The IS staff will attempt to notify all users of credible virus threats via e-mail or telephone messages. Because this notification will automatically go to everyone in the organization, employees should not forward virus warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.

As stated, it is the responsibility of all City of Livonia network users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

- Do not open unexpected e-mail attachments, even from coworkers.
- Never open an e-mail or instant messaging attachment from an unknown or suspicious source.
- Never download freeware or shareware from the Internet without express permission of the IS department.
- If a file you receive contains macros that you are unsure about, disable the macros.

Notify the help desk of suspicious files

If you receive a suspicious file or e-mail attachment, do not open it. Call the City’s Information Systems Department at extension 2150 and inform the support analyst that you have received a suspicious file. The support analyst will explain how to handle the file.

If the potentially infected file is on a disk that you have inserted into your computer, the antivirus software on your machine will ask you if you wish to scan the disk, format the disk, or eject the disk. Eject the disk and contact the help desk at extension 2150. They will instruct you on how to handle the disk.

After the support analyst has neutralized the file, send a note to the person who sent/gave you the file notifying them that they sent/gave you a virus. (If the file was sent via e-mail, the antivirus software running on our e-mail system will automatically send an e-mail message informing the sender of the virus it detected.)

If the file is an infected spreadsheet or document that is of critical importance to the City of Livonia, the IS department will attempt to scan and clean the file. The IS department, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on the City of Livonia computers.
Network User
Purpose: To document our Network User Id Policies.
Description:
Unique User ID's and passwords are to used identify authorized users of computer resources at the City of Livonia.
User ID's will generally be made up of the user's first initial of their first name with their last name as outlined in Information Systems Department Policy IS-001.
User ID and passwords are not to be shared with anyone. Employees are expected to protect their individual User ID and password from unauthorized use. The User ID and password is meant to be a unique identifier. The employee's department head must authorize a request in writing for a User ID or the new User ID will not be issued. All requests for e-mail and Internet access must be submitted on the appropriate form as approved by the Civil Service Commission.
Passwords will be set to expire every ninety (90) days. This is to protect the confidentiality of passwords. The system will remind a user in advance that their password is about to expire and give them the option to change it at that time. The system will keep a history of at least the past ten (10) used passwords by user and will not allow the user to reuse a previously used password. Passwords must be a minimum length of 6 characters and/or numbers. Passwords should be chosen that are not easy for someone else to guess. Examples of poor passwords would include family member names, favorite hobbies, birthdates, and pet names. Best passwords will include multiple words with numbers or even non-words with numbers.
If a user suspects that someone else may know their password, they are to contact the Information Systems Department.
When an employee leaves a department, it is the department head's responsibility to notify the Information Systems Department in order to have that users access disabled.
Passwords are set to be automatically disabled if there are three repetitive attempts to login with an invalid password.
Computer Software
Purpose: To document our Computer Software Policy
Description:
Standard Software Packages
The City has standardized on to the following software to be used on personal computers:
Operating System - Microsoft Windows
Word Processor - Microsoft Word 2000
Spreadsheet - Microsoft Excel 2000
Database - Microsoft Access 2000
Antivirus - Norton Corporate Edition
079 Livonia, MI – Web-Based Mail Systems Policy

Web Based Mail Systems
Purpose: To ban the use of external Web Based E-mail Systems in order to protect the security/integrity of the computer network.
Description:
Web based e-mail systems like hotmail and yahoo mail have become very popular on the Internet. Unfortunately, these systems have created a threat to the City’s computer network. The City has built a layered approach for protection against viruses. All City e-mail and attachments passes through the following checks:
1. The Firewall - where unsafe attachment types are removed
2. A SMTP Filter – where the e-mail and attachments are scanned for viruses and spam
3. An additional Spam Filter – where e-mail is checked for SPAM, valid email addresses, etc.
4. The Workstation – where the final scan for viruses occurs.
Unfortunately, external web-based e-mail by-passes layers 1-3 above and relies exclusively on the Workstation anti-virus scan. This by-pass creates a large opportunity for viruses and other inappropriate content to infect a computer on our network and then spread.
Since the City’s Internet Access Usage and E-mail policy, as approved by the Civil Service Commission and signed by all employees, states “Internet access and E-mail is provided for the purpose of conducting city business” and since the City provides E-mail accounts for the use of authorized employees, these services should not be needed.
Bases upon this situation, City Employees are not to use external web based email systems. This does not apply to the City e-mail system. The Information Systems Department will also be blocking these services as much as is possible at the firewall level.
Wireless Access Points
Purpose: To restrict the implementation of wireless access points in order to protect the security/integrity of the computer network.
Description:
Wireless Access Points (WAP) provide an easy way for computers to link to the City’s computer network, but if not implemented properly, these devices become and open gateway to the City’s network and data. These devices typically use protocols like 802.11a, 802.11b or 802.11g. As a result of the risks involved with these devices, the Information Systems Department has set a minimum standard for securing these devices and must approve any access point before it is purchased or deployed.
The standards are:
• Must have all passwords changed from the defaults.
• Must have a minimum of 40-bit Shared Key Encryption set.
• Must have the Broadcast WLAN Service Area Name (ESSID) set to off.
• Must use WPA.
• If possible, should use Radius to authenticate the user to the network before allowing access.
Because of the nature of this technology, these standards are expected to change in order to provide safe access to our network.
Instant Messaging and Peer to Peer File Sharing

Purpose: To restrict the use of Instant Messaging (IM) and Peer to Peer File Sharing (P2P) in order to protect the security/integrity of the computer network.

Description:
Two technologies that have become popular on the Internet are Instant Messaging (IM) and Peer to Peer File Sharing (P2P). Both of these technologies first became popular with the teens chatting with their friends and sharing music files. Both of the technologies are very insecure and if used, would expose our network and data to a number of vulnerabilities. Because of the inherent flaws in these technologies, the City of Livonia bans the use of these items and the Information Systems Department will do everything possible to not allow them. All users must not load IM or P2P clients on their personal computers. If discovered on their machines, these clients are to be immediately removed and the Information Systems Director will be notified.
Firewall Security Policy
Purpose: To define basic policies in regards to Firewall Configuration.
Description:
These are the general rules for the City’s Firewall
Allow NTP Outbound
Allow FTP Outbound
Allow SMTP Inbound and Outbound
Inbound should be directed from xxx.xxx.xxx.xxx=>xxx.xxx.xxx.xxx
Scan for Viruses
Scan for SPAM
Real-time Blacklist sbl-xbl.spamhaus.org
Allow HTTP Outbound

Do Webcontent Filtering Blocking
Adult/Sexually Explicit
Advertisements
Chat
Criminal Skills
Drugs, Alcohol, & Tobacco
Gambling
Glamour & Intimate Apparel
Hacking
Hate Speech
Personal & Dating
Remote Proxies
Violence
Weapons
Web-Based E-mail

Allow OWA using ssl
Directed from xxx.xxx.xxx.xxx => xxx.xxx.xxx.xxx
Allow HTTP Outbound to xxx.xxx.xxx.xxx, xxx.xxx.xxx.xxx, xxx.xxx.xxx.xxx, xxx.xxx.xxx.xxx
Allow HTTP Outbound for xxx.xxx.xxx.xxx (City Clerk Public) only to:
xxx.xxx.xxx.xxx City Website
xxx.xxx.xxx.xxx City Ordinances Website
Allow DNS Outbound
Allow DMC Support from xxx.xxx.xxx.xxx Port yyyyy (Normally Disabled)
Allow License Manager from Any Trusted or Any Optional on port yyyyy
Allow Windows Media Inbound xxx.xxx.xxx.xxx => xxx.xxx.xxx.xxx ports UDP
zzzz, TCP zzzz, TCP zzzz
Allow Windows Media Outbound ports UDP zzzz, TCP zzzz, TCP
PC Anywhere for Housing from xxx.xxx.xxx.xxx / xxx.xxx.xxx.xxx to
xxx.xxx.xxx.xxx => xxx.xxx.xxx.xxx Ports UDP zzzz, UDP zzzz, TCP zzzz, TCP zzzzz
Allow HUD Outbound Ports TCP zzzzz-zzzzz
Allow PPTP RDP Inbound Port TCP zzzz
Allow Accounting VPN Inbound to xxx.xxx.xxx.xxx and Logos.net
COUNTYWIDE POLICY
ON
Managing Information and Technology Assets
Purpose
Information assets including hardware, software, and data are some of County’s (the County) most valuable assets. This policy exists to ensure the security and proper management of these assets.
Definitions
Information Services – The Information Services Division of County
Information assets – Hardware, software and data
Resources – Assets that support a system including personnel, funds and equipment
Infrastructure – The communications system that includes, but is not limited to, the backbones, data lines, routers, switches, wireless access points, access methods and protocols
Network services – Services commonly provided by the network including, but not limited to, authentication, directory services, DHCP, DNS, e-mail and web hosting
County network – All computers and networks that receive infrastructure or network services from the County
Intranet – The County network segment available only to internal users through a web browser
Public access system – A computer, program, network or data system available for public use or intended to be accessed by individuals without requiring County authentication
Policy
1. This policy, along with the supporting standards and procedures, is to be maintained and kept current by Information Services and published on the County Intranet.
2. Acquiring and Managing Information Technology Assets
   2.1. Information Services must maintain a database of all significant County information assets.
   2.2. New information technology and/or modifications to existing technologies must be justified by a strong business case or operational necessity and must be supported by adequate resources. Approval is the responsibility of Information Services in cooperation with the department director/elected official or their designee.
   2.3. All information technology, hardware, software, data and services must be acquired, created and managed according to Contracts and Procurement policy and Information Services standards.
   2.4. Only legally licensed software may be installed and/or used.
   2.5. All software installed or used must be officially approved. Approval is based upon compatibility, standardization, security and other justifiable and valid technical and business concerns. A list of approved software will be maintained by Information Services on the Intranet. Approval is the responsibility of Information Services in cooperation with the department director/elected official or their designee.
   2.6. Information Services has sole responsibility for the County network. All connections to the County network must be provided by Information Services.
   2.7. Information Services must provide infrastructure and network services sufficient to meet County business needs.
   2.8. Equipment connected to the County network must be owned by the County and certified by Information Services.
   2.9. Information technology systems, hardware and software, must be maintained by properly trained and approved personnel, including non-County personnel such as contractors. Approval is the responsibility of Information Services in cooperation with the department director/elected official or their designee.
   2.10. County information assets must be reasonably protected from inappropriate access.
   2.11. Information must be stored and backed up in a manner fitting expected accessibility, integrity, confidentiality, longevity and recoverability needs and in accordance with County records management policies.
2.12. Information security incidents and vulnerabilities must be reported and handled appropriately.
2.13. Public access systems must be sufficiently protected against inappropriate use.

3. Using Information Technology Assets
3.1. All users are required to comply with the County's Information Services standards and procedures. The monitoring of such compliance is the responsibility of management.
3.2. All employees, as part of new hire and biannual training, are to be made aware of their responsibilities with respect to their use of information systems and data. This includes, but is not limited to, applicable regulations and County policies.
3.3. All persons, functioning in any capacity, utilizing County information systems must receive adequate training to ensure that they do not compromise security or system integrity.
3.4. Users of confidential and/or sensitive information are responsible for the proper security of that information.
3.5. The County reserves the right to access any information that is stored or processed on County equipment, connected to the County network, or created for the County. Employees have no right to or expectation of privacy regarding material on any electronic media. All such media are subject to periodic inspection or audit without notice.
3.6. Personal use of the County information systems, such as computer equipment, network, Internet and e-mail, is a privilege and not a right. As such, the privilege may be revoked at any time and for any reason. Limited personal use is permissible so long as it: (a) does not interfere with worker productivity and (b) does not preempt any County business activity. No personal use may be made by, or on behalf of, any organization or third party.
3.7. Using County systems for private business use of any type or amount is prohibited. Department directors/elected officials may adopt written policies to allow the limited use of County systems for affiliated non-profit organizations which provide significant support for County programs.
3.8. Acceptance of this policy along with the supporting standards and procedures is required for use of County information assets. Any use constitutes acceptance.

4. If Information Services does not concur with the department director/elected official regarding any decision under this policy and the department/offic e desires to proceed, the request shall be brought before the Executive Committee for final resolution. The functions of the elected officials set out in state statutes shall be taken into consideration during this process.

5. Failure to comply with this policy with its supporting standards and procedures may result in disciplinary action.

Standards and procedures will be modified as the County adopts new technologies and processes. Always refer to the standards and procedures when researching a question or making an information technology decision.
084 Branford, CT – Web Site Policy

Branford WEB site at www.branford-ct.gov

Purpose
To establish a policy regarding the Town of Branford’s web site such that responsibilities are clearly understood. The web site is www.branford-ct.gov

Policy
The Information Technology Director has the responsibility for the design, standards and consistency in format, look and availability of the Town’s website. Department Heads are individually responsible for the accuracy and timeliness of all content pertaining to their department. Departments are expected to post such items as: Agendas, minutes and meeting notices in a timely and legal matter. Initially Information Technology will do the posting at the request of the department. However, when a process has been established and training has occurred, departments will have the direct responsibility for all department postings and their removal as appropriate. The Branford site is to be the “site of choice” when services provided by an outside vendor are equal to or less than those provided by the Town. Information Technology will work with outside vendors as time allows to help ensure a department’s web objectives are met. When appropriate and possible Information Technology will “host” an entire web site, developed for a department, on the Town’s servers.

Departments are responsible to bring to the attention of Information Technology all current web related expenses and any presently planned (or when planned in the future). It may be we can be of help in the design, hosting or development itself, thus saving money.
Desktop Personal Computers

Purpose
To establish a policy regarding the Town of Branford’s Personal Computers (PC’s) such that end users know what to expect as the “standard” configuration and operation.

Policy
Information Technology Director has the responsibility for all computers, software and peripheral computer devices for the Town of Branford, exclusive of the Board of Education Department. We are presently a “Microsoft” environment with a few legacy applications continuing to be run on the IBM AS/40. It is the stated policy to move to a 100% Microsoft server/Intel environment as soon as possible and practical. Desktop computers will come with the following “standard” software unless a department head wishes something different;

• Microsoft Office Professional (Word, Excel, PowerPoint, Outlook, Explorer, Publisher and Infopath)
• Department unique applications (such as Geoplan, Vision, GIS-ESRI ARC Reader, COTT, etc.)
• “O” drive access for all shared information such as; Policies, HR information, etc.
• CITRIX Login where appropriate
• Personal Data Assistant (PDA) support software where appropriate
• Game software will NOT be delivered with the PC
• Antivirus software (set to run automatically)

Town “Domain” based PC’s will be defaulted to the main file server at the Town Hall (TH-FS02). This will provide for automatic daily back ups for all files so stored. Should a user save a file to the local drive on their PC, back up of the data will not be the responsibility of IT. Software will be configured to;

• “Empty” the “Deleted Items” in Outlook when the user logs off of the application. Trash cans should be emptied periodically for all other applications.
• Set Explorer to www.branford-ct.gov as the “home page”. Cookies and internet temporary files will be deleted at logoff.
• The User’s ID will be the 1st initial of their 1st name and full last name @branford-ct.gov for all PC’s except; BOE, Police and Fire.
• The signature will be created for all employees when the PC is installed to read;

Name
Title
Town of Branford
“Work address”
Branford, CT 06405
Telephone number (direct if possible)
Visit us at www.branford-ct.gov

Outlook data (emails and their attachments) will be stored online for a maximum of two (2) years. Users are encouraged to “archive” any emails and to save any attachments they wish to keep beyond this point. This action is necessary to stay within our license agreement and to avoid a “hard stop”. Department Heads and designees will be provided with remote sign on capability allowing them access to their files and applications from home, should they so desire. All applications they are authorized access to from there desktop in their office will be available from “home” through our CITRIX server. NOTE: There are a few legacy applications (mostly DOS based) that cannot be accessed through CITRIX remotely.

Thin Client PC’s will be the PC of choice whenever it is possible to deploy this type of PC verses one where the application software is loaded at the desktop. Public access terminals will default to “Thin Client”. All users are to log off of the network daily. It is not necessary or recommended that users turn the PC off on a daily basis. We have software that “inventories” PC application software and hardware after hours when the PC is left on. Additionally, CITRIX accessed files that are “open” during system backup (between 10 p.m. and 7 a.m.) cannot be backed up. It is recommended you turn off your display off daily such that an eerie glow does not emanate after hours from the display. When the user is to be
away for more than a day, the PC is to be powered down. Failing to log off locally may result in the user’s work not being backed up. On a building basis all printers within the building will be addressable by all PC’s (except for public PC’s) such that if a user wishes to output to another printer, they may easily do so. The default printer will be set to the desktop printer whenever one is present.
086 Branford, CT – FOI Requests Policy

Requests for information under the FOI laws.
PURPOSE
To ensure the process of obtaining information stored on the Town’s computer systems is consistent in practice and in assessing fees for the service.
POLICY
All requests for FOI type information are to begin in the Selectman’s office. The Selectman’s Assistant is responsible for taking down the request on a written form (provided by Information Technology (IT)) and seeing that IT receives a copy of the request. IT will then “quote” on the request after assessing the scope of effort and time required to complete it (if possible). This information will be sent back to the Selectman’s assistant if the cost is greater than $10 such that the requestor can be informed of the quote. The quote will be developed within 48 hours of receiving the request form. Information Technology will work to “turn around” all requests within four (4) business days of receiving them. Media requests will be produced on and are limited to; CD’s, paper and electronically transmitted files. Tape and Floppy requests will not be honored.
087 Branford, CT – Downtime Policy

Downtime Policy
Purpose
Branford’s Information Technology Department is committed to ensuring reliable information technology services. In order to meet this objective, systems may need to be taken offline to maintain or improve system performance, safeguard data, or to respond to emergency situations. The goal of this policy is to explain those circumstances during which downtime may occur, anticipated durations of downtime events, and procedures for notifying affected users.

Planned Downtime
From time to time, it will be necessary to make systems unavailable for the purpose of performing upgrades, maintenance, or housekeeping tasks. The goal of these tasks is to ensure maximum system performance and prevent future system failures. The following activities fall within the definition of Planned Downtime:

- Application of patches to operating systems and other applications in order to fix vulnerabilities and bugs, add functionality, or improve performance.
- Disk defragmentation, disk cleanup, and other general disk maintenance operations.
- Required upgrades to system physical memory or storage capacity.
- Installation or upgrade of applications or services.
- System performance tuning.

In the event that any of these activities will require downtime to perform, every effort will be made to perform the procedure during off-hours in order to minimize the impact on those who use the affected systems or services.

On occasion, it may be necessary to have Planned Downtime during regular business hours, namely if outside personnel are required to perform more elaborate procedures. If this is the case, then this Planned Downtime will be communicated to identified users of affected resources using the Notification of Downtime mechanism described below.

Emergency Downtime
Unexpected circumstances may arise where systems or services will be interrupted without prior notice. Every effort will be made to avoid such circumstances. However, incidences may arise involving a compromise of system security, the potential for damage to equipment or data, or emergency repairs. While this type of downtime is not anticipated, if the affected system(s) cannot be brought back online within thirty (30) minutes, affected users will be contacted via the telephone and then called again as soon as the system(s) are back up.

All downtime announcements will provide the following information:

- Systems and services that are affected, as well as suggested alternatives to them (if any).
- Start and end times of the Planned Downtime period, or estimated time to recovery in the event of Emergency Downtime.
- The reasons why the downtime is taking place.
- Any ongoing problems that are anticipated as a result of the downtime event.

Requests for Availability
If you foresee critical need of a system during a period of Planned Downtime, then contact myself, Pete Eirich or Joe Abbatello in advance to make an appeal. The utmost effort will be made to reschedule the downtime or make alternative arrangements for required resources.
Information Technology’s policy relating to new hires and employees leaving the Town’s employment.

PURPOSE
To clearly set responsibilities associated with technology access when is hired or leaves the Town’s employment.

POLICY

Employee Hiring
1. The Human Resources department will inform IT as soon as possible by email when a new employee is starting work for the town with their start date and department.
2. IT will contact the appropriate department head to determine technology requirements (hardware and software) and see that they are in place by the start date.
3. The department head will inform IT if documents from the last person who held the position should be moved to the new employee’s personal folder (H drive) from the shared department drive.
4. IT will create the new user on the system, including assignment of username and password.
5. IT will create the new employee’s personal folder, email account and add the new employee to any department specific email distribution lists and update the internal phone directory if appropriate.
6. IT will then contact the department head by email stating that the new employee setup is complete.
7. The new employee is to contact IT such that IT can instruct the new employee on the technology including their username and password. It is at this time IT will also instruct Town Hall based employees on their phone usage.

Employee Exiting
1. The Human Resources department will inform IT as soon as possible by email when an employee is exiting town employment with their exit date.
2. The department head is to work with the exiting employee to gather any necessary information from the exiting employee’s email account.
3. IT will verify with Human Resources on the “exit date” that the employee has left the employ of the Town.
4. IT will then move the exiting employee’s “H” drive documents (Word, Excel and PowerPoint) to the department’s shared folder in a sub-folder with the name of the exiting employee.
5. IT will remove the exiting employee’s user account from the system, including all system distribution lists, and all application software.
6. The exiting employee’s email box will be deleted and if the employee is Town Hall based their voicemail box and extension will be reset to the generic setting.
7. IT will then contact the department and Human Resources by email stating that now, past employee has been removed from the system.
Technology Usage Policy

PURPOSE
To establish a policy regarding the proper use of the computer, electronic, voice and telecommunication technology system (the “system”) of the Town of Branford, Connecticut (the “Town”) by each Town officer, employee or any other person or entity authorized by the Town to use the systems (referred to as “user”).

POLICY
The Town's system, including e-mail, voice mail, facsimile communication and Internet access, are Town property intended for official Town business purposes, and are not to be used for other purposes. Incidental and occasional personal use of the system that is not inconsistent with this policy may be permitted, but shall not interfere with the user's access by others or performance of his or her job duties. The Town has the right to monitor, intercept and evaluate any and all usage of the Town's system as permitted by law. No user has any right or expectation of privacy or ownership in anything that is created, sent, received or stored by computer (including e-mail), fax or voice mail. Each user is responsible for using the Town's system, resources and service in an efficient, effective, ethical and lawful manner and in accordance with applicable statutes, ordinances and this policy. This policy applies to all users of the Town’s system, wherever the users are located. The following rules apply to the use of the Town’s system:

1. Users must comply with all laws governing intellectual property, such as software licenses and copyrights.
2. The Town's system, including access to networks, is to be used for recognized public purposes of the Town and shall not be used for the transmission or storage of private advertisement, solicitations, promotions, destructive programs, political material or for any unauthorized use.
3. Users shall not use the system, including access to the Internet, to view and/or disseminate indecent or otherwise inappropriate information, material or messages. Users shall not view and/or disseminate information, material or messages that may be hostile or offensive to another on the basis of sex, race, religion, color, national origin, sexual orientation or disability. Indecent, vulgar, harassing, fraudulent, intimidating or otherwise inappropriate unlawful material may not be sent by e-mail, voice mail, fax or other form of electronic communication, or displayed on or stored in the Town’s system except by law enforcement officials during official investigations. While users cannot always control what material they receive, users who do receive any such material from another user or third party must not retransmit or forward such material to any other person and shall immediately notify the Town’s human resources director of the existence of such material.
4. Users must check their individual, and if applicable, their departmental, e-mail and voicemail on a daily basis and are expected to reply within 24 hours. It is suggested that e-mail and other electronic documents should be drafted with the same degree of care as any other written communication. Except as permitted or required by law, anything transmitted electronically, by facsimile or e-mail, is not confidential, and may be reviewed by others.
5. Users may not purchase or install software in their individual computers or the network without first receiving express written authorization to do so from the Information Technology department head.
6. Email messages from individuals who are not employees or officers of the Town may not be altered or forwarded to any other person or entity without the express or implied permission of the sender.
7. Each user will be issued a user sign-on identification and an “initial” password by the human resources department that is to be used only by that user. Users should regularly change their user passwords for security purposes and are responsible for safeguarding them. Individual passwords should not be printed, stored online or given to others. Except for official monitoring functions, users are responsible for all transactions made using their passwords.
8. The ability to connect to other computer systems through the network does not imply a right to connect or to make use of those systems unless specifically authorized by the operators of those systems.
9. Access to and use of the Internet is restricted to Town related business only, by authorized employees. A user’s Internet activities may be logged by a surveillance system and reviewed by the information technology department, if so directed by the first selectman or human resources director.
10. Information or electronic communications using the Town’s system are subject to the FOIA of the State of Connecticut and may also be subject to disclosure in legal proceedings.

11. The Town has an obligation to retain certain information stored on the IT system in accordance, General Letter 98-1, “Electronic and Voice Mail: A Management and Retention Guide of State and Municipal Government Agencies” issue by the State of Connecticut Office of the Public Records Administrator and State Archives as it may be amended from time to time. While many email messages are temporary communications that are non-vital and may be routinely discarded, email messages that are more formal or substantive must be retained by the Town in accordance with state standards. Examples of such messages include, but are not limited to, messages related to policies, decision making, material connected to a specific case, application, or business matter, contracts, part of a record, or business functions. Users who are uncertain whether a specific email message must be retained should err on the side of caution and retain it.

12. The Town reserves the right to monitor its IT system at any time, without notice, to ensure they are being used for Town purpose only. The Town’s monitoring policy will be in accordance with all applicable federal and state laws, including CGS Sec. 31-48d.

EMPLOYEE ACKNOWLEDGEMENT

I acknowledge that the Town has provided me with the notice required under CGS 31-48d indicating that it may monitor my use of its IT system. I have read and understand the above procedures and policy, including the Town’s right to monitor my use of the IT system, and consent to it. I understand that the Town has provided me with access to IT system and will assign an email address and/or voice mailbox to me based upon my representation that I will abide by this policy. I understand that any violation of this policy may subject me to discipline, up to and including termination.
To properly align itself with the Commonwealth of Pennsylvania, the County of Butler hereby adopts, in principal, the Information Technology Bulletins currently published by the Governor's Office of Administration/Office for Information Technology. Although some of the Commonwealth’s policies specifically reference OIT initiatives, the County has gleaned the following portions of these ITBs as a basic policy set.

The County’s Department of Information Services (IS) is responsible for the policies, guidelines, and standards governing information technology investments by all agencies under the Commissioner’s jurisdiction, based on direct input and advice from County departments and Row Offices. Effective immediately, IS resources will be managed, planned, and acquired in accordance with the direction set forth in this document and subsequent revisions that may be made.

The County will govern IS by policy and performance not bureaucratic processes and rules. To ensure the Commissioners’ program priorities are achieved through an effective and proactive approach. IS correlates all activities based upon these standards:

* Maximize County Assets
* Effectively Manage Investments
* Safeguard County Assets
* Improve Public Access to Government Information & Services
* Enable e-Government when appropriate

IS is responsible for developing and promulgating countywide policies and standards governing the management and use of the County’s information technology investments.

The Commissioners’ Chief Clerk has asked IS to review all agency technology related budget submissions, and provide technical and budgetary recommendations for each technology project. Ultimately, all funding decisions rest solely with the Commissioners and the Chief Clerk.

802 COMPUTER TECHNOLOGY

1. Desktop computing and networking technology are resources critical to the effective and efficient operations of local government and must be managed to provide a flexible and responsive computing environment, support communications and exchange of information, and are consistent with accepted industry standards.

2. Significant problems have been encountered due to offices running different versions of operating system software, office productivity suite software and e-mail systems have lead to the inability to easily exchange or share documents and effectively send and open attachments to e-mail messages. This has also added to the cost of ownership for IT technical staff to support multiple products, different version levels, and increased training costs.

3. IS will coordinate the development of all desktop technology policies and standards and will be responsible for managing their implementation.

4. It is the policy of IS to ensure and promote a countywide expansion of desktop computing and network based technology through the development, provisioning, implementation, and coordination of the following functions: hardware and software standards, development and implementation of a IT modernization plan, programs to minimize cost of IT ownership, IT education programs, and technical assistance.

5. As with other fixed assets of the County, personal computers should be kept in physically secured areas to minimize the risk of theft or unauthorized access.

6. Original copies of software stored on a hard disk, backup software, primary programs, and data files maintained on removable media and documentation must be kept in a physically secure area.

Hardware Standards for Desktop Computing Devices

- Dell Optiplex Computers
- Toshiba; Dell Latitude Computers
Black & White and Color Printers
Hewlett Packard LaserJet; Dell printers

803 DESKTOP SOFTWARE

1. Desktop software standards assist with the effective deployment, utilization and management of IT resources and provide the following benefits:
   1.1 A flexible, easily adaptable, distributed computing environment
   1.2 A computing environment that is responsive to the increasing and ever-changing service demands and business requirements of County agencies
   1.3 Ensure computing resources are used as efficiently and effectively as possible
   1.4 A distributed computing resources to enhance productivity by providing tools that are easy to use, integrate seamlessly, minimize application disruptions, and enhance system availability
   1.5 Improved interaction and communication between agencies and easier exchange of information and documents created with application software
   1.6 Allows County and Commonwealth agencies to use desktop software and collaboration tools in an effective and efficient manner.
   1.7 An overall reduction to an organizations total cost of IT ownership (reduced training requirements for end users and technical support staff, a decrease in technical problems, minimized system downtime, etc.)

2. In establishing the products identified as county-wide standards for desktop computing, IS is developing support for County agencies, including, but not limited to: help desk support, technical consulting services, and training.

3. To minimize problems and ensure countywide consistency and compatibility, agencies may not initiate upgrades beyond the standard software products specified.

4. The standards initiative will migrate all affected desktop computing devices to consistent version levels of these products over a three-year period. In the past year IS has been implementing security procedures that limit the installation of software on desktop computers to assist in enforcement of these standards.

Software Standards for Desktop Computing Devices

Desktop Computing Software Category Products

Desktop Operating System
- Windows XP Professional (CAL)
- Office Productivity Suite
- Microsoft Office XP Standard and Professional
- Microsoft Office 2000 Standard and Professional

Word Processing
- Microsoft Word 2002 and Microsoft Word 2000

Spreadsheet
- Microsoft Excel 2002 and Microsoft Excel 2000

Graphics/Presentation
- Microsoft PowerPoint 2002 & PowerPoint 2000

Desktop Database
- Microsoft Access 2002 and Microsoft Access 2000

804 SOFTWARE USAGE

1. Butler County has purchased licensed copies of computer software from a variety of publishers and has placed them on computers within the County. No copies, aside from a backup, of the software or its documentation will be made without the express written consent of the software publisher.

2. The use of software obtained from any other source could present security and legal threats to the County, and such use is strictly prohibited.

3. The unauthorized duplication or use of copyrighted software or documentation is a violation of the law and is contrary to established standards of conduct for Butler County employees. Butler County will not tolerate any employee making or using unauthorized copies of software, including for use by third parties.

4. No employee may use or distribute personally owned software on Butler County's computers or networks. Such software threatens the integrity and security of the organization's computers and networks.

5. A variety of software is available on the Internet. Some of this software, called "freeware" or "shareware," is available free of charge for limited use and may be downloaded to your computer only with the prior written approval.
6. No employee shall install or distribute software or software upgrades for which the County lacks the appropriate license.
7. Butler County reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorized copies of software. All copies of software that is obsolete or for which the County does not have an appropriate license will be removed from the County computers and destroyed.
8. Employees may be held responsible for the existence of any software on their computer for which the organization lacks the appropriate licenses.
9. Anyone found in violation of any of these policy statements is subject to disciplinary action up to and including termination of employment with the County of Butler.

805 ELECTRONIC MAIL
1. The County of Butler provides electronic mail (e-mail) to employees for County business purposes.
2. All electronic messages created and stored on Butler County computers or networks are property of the County of Butler and are not considered private.
3. E-mail messages should contain information related only to government business.
4. In using the e-mail system, the employee waives any claims to privacy.
5. Butler County retains the right to review all employee e-mail and is able to re-create e-mails even if both sender and reader have deleted the e-mail.
6. E-mail should not be used to transmit confidential information without advice from the county solicitor and must be encrypted to protect the information.
7. Incoming messages will be scanned for viruses and other malign content.
8. Use of electronic mail services for purposes constituting clear conflict of Butler County interests or in violation of Butler County information security policies is expressly prohibited, as is excessive personal use of email.
9. Messages that contain sexually explicit materials, obscene and discriminatory language or solicitation for commercial ventures or religious causes are prohibited.
10. Employees should not use their government e-mail addresses in connection with private online portals, chat rooms, bulletin boards, or to receive personal material, such as, but not limited to, information on stocks and bank records.
11. Limited personal use is acceptable as long as the overseeing Row Officer and/or Department Head approve it and doesn't interfere with the completion of work.
12. Use of Butler County e-mail to participate in chain letters or to advertise items for sale is not acceptable.
13. The use of email in any way to facilitate the conduct of a private commercial purpose is forbidden and is subject to disciplinary action.
14. Users must not allow anyone else to send email using their accounts. This includes their supervisors, secretaries, assistants and any other subordinates.
15. Anyone found in violation of any of these policy statements is subject to disciplinary action up to and including termination of employment with the County of Butler.

806 INTERNET
1. Employees must obtain approval from their Row Officer/Department Head and the Chief Clerk to be given Internet access.
2. All users who require access to Internet services must do so by using county-approved software and Internet gateways.
3. All other forms of Internet access (such as via dial-out modems) from sites connected to the County network are prohibited. Employees must not circumvent the firewall.
4. All access to Internet services is logged. Any attempts to access forbidden sites will be reported to your manager.
5. Access and use of Internet through a County-supported connection is authorized for the purpose of conducting County business. Use for personal reasons other than incidental and occasional personal use is not acceptable. Use for personal gain or for the conducting of business that is not County related is strictly prohibited.
6. While on the Internet, the Butler County name will be associated with any communication that is sent. Therefore, commentary that is inconsistent with Butler County policy or personal opinions of the sender that reflect poorly on Butler County are unacceptable and must be avoided.
7. When expressing opinions or responding to discussion topics, unless the user is authorized to speak on behalf of Butler County, the following disclaimer must be added to all communications:

“The opinions expressed are those of the writer and not of Butler County.”

8. Users must insure that all communication sent through the Internet in pursuit of County business is clear as to meaning and that such communication does not violate any applicable law or regulation.

9. The County reserves the right to block any sites that are sexually explicit, obscene, or discriminatory. To gain access to a blocked site, the issue should be raised with your manager and IS management.

10. Some Internet communications protocols have been blocked or redirected. If you have a business need for a particular protocol, you must raise the issue with your manager and IS management.

11. The downloading or transmitting of sexually explicit materials, obscene and discriminatory language, unlicensed software, or software upgrades not approved by IS is prohibited.

12. Anyone found in violation of any of these policy statements is subject to disciplinary action up to and including termination of employment with the County of Butler.

807 NETWORK SECURITY

1. All information traveling over County computer networks that has not been specifically identified as the property of other parties will be treated as though it is a County asset.

2. It is the policy of the County to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

3. Information security administrators are responsible for ensuring that appropriate computer and communication system security measures are observed and for making sure that all users are aware of County policies related to computer and communication system security.

4. Users are responsible for complying with this and all other County policies defining computer and network security measures. All users share an obligation to keep their use secure on a day-to-day basis.

5. The computer and communications system privileges for all users, systems, and independently operating programs must be restricted to a need-to-know basis. Privileges must not be extended unless there exists a legitimate business-oriented need.

6. Default user file permissions must not automatically allow anyone on the system to read, write, or execute a file.

7. Users with microcomputers are responsible for administering an approved screen saver program securing access to their machine's hard disk drive and setting passwords for all applications and systems software that provide the capability.

8. System administrators will restrict a user’s access to the County computer and communications network based on specific user requirements. Sufficient restriction must be in place to prevent a user from logging in to a certain computer then gaining access to other computers within the network.

9. Requests for new user IDs or privilege changes must be made in writing and approved by the user's supervisor before a system administrator fulfills these requests.

10. Individuals who are not County employees must not be granted a user ID or otherwise be given privileges to use County computers or communications systems without proper authorization.

11. All access for a user ID will be revoked after a specified period of no use. The recommended period is every thirty (30) days.

808 COMPUTER/NETWORK USER ID

1. All users must be positively identified prior to being able to use any multi-user computer or communications system resource.

2. Requests for new user IDs or privilege changes must be made in writing and approved by the user's supervisor before a system administrator fulfills these requests.

3. User IDs must be unique and identifiable by user.

4. Once a User ID is deleted, it cannot be re-issued.

5. IS must maintain a record of all User ID issued. This record must identify the person associated with the User ID and the timeframe during which the User ID is/was valid.

6. Users will always need to enter their password manually to unlock their workstation.

7. Incorrect password attempts must be strictly limited to prevent password-guessing attacks. Upon three (3) consecutive, unsuccessful attempts to enter a password, the involved user ID must either be suspended until reset by a system administrator or temporarily disabled for no less than three (3) minutes.

8. If there has been no activity on a personal computer for a certain period of time (maximum of 15 minutes), the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password.
9. Each department or agency should define a maximum inactivity timeout before the computers are automatically locked down and require a password to activate.

10. The computer and communications system privileges for all users, systems, and independently operating programs must be restricted to a need-to-know basis. Privileges must not be extended unless there exists a legitimate work-oriented need.

11. System administrators will restrict a user’s access to the County computer and communications network based on specific user requirements. Sufficient restriction must be in place to prevent a user from logging in to a certain computer then gaining access to other computers within the network.

12. IS will set-up and maintain a user list on each file server, mid-range computer and network that resides within IS.

809 COMPUTER / NETWORK PASSWORD

1. All users must be positively identified prior to being able to use any network connected computer or communications system resource. Positive user identification involves both a unique user ID (assigned by IS) and a password.

2. Passwords must be comprised of a minimum of 8 alphanumeric characters.

3. Passwords must be changed by the user every 30 (preferred) to 90 days. IS will automatically force a password change based on policy and procedures.

4. Users must not construct passwords that are identical (or substantially similar to) passwords they have previously employed. Password will be retained by the system for a minimum of 3 prior passwords to prevent the re-use of prior passwords.

5. Users must choose passwords that are difficult to guess: Passwords must NOT be related to one's job or personal life. Do not use a car license plate number, a spouse's name, or an address. Passwords must not be a word found in the dictionary. Proper names, places, technical terms, and slang must not be used.

6. Passwords must not be written down and left in a place where unauthorized persons might discover them. No passwords should be posted in or around a user's work area.

7. Passwords must never be shared or revealed to anyone else besides the authorized user regardless of the circumstances. When users need to share computer resident data, they should use electronic mail, public directories on local area network servers, or other mechanisms.

8. All passwords must be immediately changed if they are suspected of being disclosed, or are known to have been disclosed, to anyone other than the authorized user.

9. All personal computers should have a boot-up password set to deter unauthorized access. The role of IS is to assist the end-user, not to choose the password.

10. It is the responsibility of each department head or row officer to maintain a secured list of user logins and passwords. Each end-user must guard his/her own password.

11. IS will not maintain any lists of passwords that have been established by the end-user. IS will only maintain passwords that have been set-up by IS, primarily on any mid-range computer system.

12. Each department that utilizes a centralized database application should appoint an application administrator to assign user passwords and security rights.

810 USER DEPARTMENT DATA BACKUP

1. User departments are responsible to ensure that magnetic files located on the local hard drive of a personal computer within their department are properly backed up.

2. It is strongly suggested that data files NOT be stores on the local hard drive or diskette, but instead be stored to the hard drive of a file server within IS. This will ensure that these files are consistently backed up by IS.

3. Backup consists of copying data files held on a hard drive to a diskette or other magnetic media. If original data files are stored onto a diskette, it is critical to make copies of these diskettes whenever a data file is updated.

4. The backup process will ensure that data files that are destroyed or corrupted due to human error or a disaster can be recovered by restoring the backup copy. The backup copies should be stored in a fireproof media container. If the data is of a critical nature, it should be stored at an offsite location.

5. It is the user department’s responsibility to determine which production files are to be backed up. As a general guideline, any software applications and data files that are stored locally should be periodically backed up and properly stored. Users that need help in establishing a sound backup routine may contact IS for assistance.
6. It is the user department’s responsibility to establish the frequency on which backups are made. Normally, backup copies should be made after data has been altered or updated on the magnetic media. IS recommends a daily backup procedure of data files used in production applications and a monthly full-system backup. If the original application program files are maintained in a secure place, they do not need to be backed up on a regular basis.

7. Departmental backup procedures should include the use of several backup versions. The department should consider keeping three backup versions, the latest (son), the preceding backup version (father) and the one prior (grandfather). The media for these backups can be recycled when a new backup is established.

8. Each set of diskettes should be clearly labeled with the following: 1) date and time of backup, 2) general description of type date backed, and 3) diskette number and total number in series (i.e. 1 of 3, 2 of 3, 3 of 3)

9. If a department utilizes a centralized database application that resides on a file server within IS, an integrated security module must be a part of the database application.

811 NETWORK SERVER DATA BACKUP

1. IS will be responsible for ensuring all files that exist on any file server or mid-range computer residing within IS will be consistently backed up.

2. A full system backup is completed on each of the file servers and mid-range computers on each Monday evening that is not a County holiday. When a holiday falls on a Monday, no backup is performed and a full system backup with the exception of the operating system is normally performed Tuesday through Friday.

3. For those departments that have a file server or other mid-range computer located within their department, it is the department’s responsibility to properly backup these systems on a regular basis. IS will assist the department in developing a sound backup routine for these remote systems, but will not be responsible to perform these backups.

4. All backup tapes or disks from any system should be stored at an off-site location in a media fireproof container. The County owns four such containers. Two are located in IS and one at the 911 Center. The media from the 911 Center should be rotated to the media safe in the IS and the media from the Government Center would be rotated to the media safe at the 911 Center.

5. Mission-Critical IT resources that should also have off-site storage include:

   5.1 Agency Business Recovery Plan (BR Plan) and Agency Vital Records
   5.2 Inventory Records: Hardware, System/Application Software, Tape/Disk Libraries, Supplies, Schematics and Floor Plans
   5.3 Master Files, Transaction Files, Database, Data Files
   5.4 Operating System Software
   5.5 Application and 3rd-Party Software, Library, Software
   5.6 Source and Executive Programs
   5.7 Security Software
   5.8 Documentation Required To Process Mission-Critical Applications
   5.9 Systems, Programming, Operations, and Run Book Documentation
   5.10 User and 3rd-Party Documentation
   5.11 Inventory of Other Materials, Supplies, Documentation Needed for Processing at an Alternate Site
   5.12 Journals, Software, Special Forms/Critical Supplies

812 DISASTER RECOVERY POLICY

1. Users must be aware of and prepared to implement a contingency plan in the event that a natural or man-made disaster causes one or more computers owned by Butler County to become unavailable for use.

2. Successful disaster recovery will be facilitated by proper compliance with the policies and procedures for data backup and recovery as outlined in the manual.

3. It is the responsibility of the user department to ensure that backup copies of any data files, departmental software or software documentation are properly maintained.

4. The following procedures must be followed in the event that a natural or man-made disaster causes one or more personal computers that are critical to the daily operations of the department and/or County to become unavailable for use.
4.1 IS shall make the determination as to what degree the Butler County Data Center is operational and report said information to the Butler County Board of Commissioners. Such determination should be made within four hours of the triggering event.

4.2 The IS shall be responsible for locating and obtaining access to a personal computer system for each user who has requested it in writing, or in the case of extreme emergency, verbally.

4.3 IS shall determine if there are personal computer systems owned by Butler County at other locations outside of the disaster area that can be used, and shall be responsible for coordinating usage among the involved users.

4.4 IS shall, if necessary, obtain personal computers from outside sources and arrange for access to these systems by users. Possible sources of equipment will include rental or loaner systems from local businesses and/or the purchase of systems from approved vendors.

4.5 IS, in conjunction with the requesting user, shall be responsible for retrieving each user’s required backup media and installing the appropriate applications and data on the obtained computer systems.

4.6 IS shall be responsible for taking appropriate steps to return each user to normal operations as soon as possible after the emergency stage of the disaster is over.

4.7 If a mid-range computer or file server is deemed non-functional, then IS will assist the County Solicitor in formulating a disaster recovery contract with a Disaster Recovery Team to provide temporary computer systems.

4.8 The IS staff will provide as many contiguous hours of data center staffing as physically possible in order to accommodate all user requests.

813 NON-STANDARD SOFTWARE POLICY

Background: Several types of software fall outside the realm of the standards list but are still necessary to the function of the various departments supported by IS. The support of this non-standard software puts a large drain on limited IS resources.

All non-standard software brings with it questions about compatibility with the operating system, the network, or other programs and whether it is properly licensed.

1. The primary non-standard software comes from vendors and government agencies that are outside the County and over which IS has little or no control. These are normally shared systems running on servers with client software on user computers.

1.1 An advantage of this software is that there is a vendor behind the product providing technical and user support. This makes it easier for IS to work with the vendor during installations and assures the users “how to” support.

1.2 A drawback is that some vendors prefer to by-pass IT when doing upgrades or making corrections to the software. This can cause problems with the computer or network and make IS troubleshooting nearly impossible.

1.3 When working with a vendor or the Commonwealth, it is imperative that IS be brought into the process early on to ensure compatibility and integrity.

2. The second type of non-standard software involves computer applications that are mainly single user programs. (Examples are: Quicken, Publisher, Print Shop, etc.). Please note that this includes both active screen savers and active wallpaper.

2.1 This is the most difficult type of software for IS to deal with because there is little or no knowledge of the software within IT, potentially leaving both the computer and the network open to difficulties.

2.2 If an agency wants to use a non-standard software application of this type, they must seek permission (or in the case of a replacement for standard package, a waiver) by submitting the request in writing to the Director of Information Technology.

2.3 The permission or waiver must include a comprehensive and well-documented business case to justify the software. Submission of a permission request will normally lead to acceptance (except in extreme cases). Submission of a waiver does not guarantee the granting of an exemption.

2.4 If permission or an exemption is issued, the agency will be required to obtain the non-standard product using its own funds through normal procurement methods.

2.5 In addition, after assisting initial installation, IS will not provide technical consulting, help desk services, or training for the non-standard, unsupported products.

2.6 If it is determined by IS that the software interferes with the operation of the computer, other software, or the network, then the non-standard software will be removed.
Acceptable Use of City Computing Resources

12.1 Purpose
The purpose of this Policy and Procedure is to define the City’s guidelines for access to and acceptable use of electronic mail (email), Internet, and Intranet access, and to define the responsibilities of City employees. This Policy and Procedure supersedes the “Acceptable-Use Policy for Computer Network and Internet Services” dated 21 August 2001.

12.2 Policy
It is the Policy of the City of Montgomery (“City”) to make email, Internet, and Intranet access available for some City employees and some contractor employees as necessary for the performance of their assigned duties.

12.3 Applicability
This Policy and Procedure is applicable to all City employees and contractor employees who access, or may access, City Computing Resources.

12.4 Definitions

12.4.1 City Computing Resources
For the purpose of this policy, City Computing Resources include the City’s computer network, Internet, Intranet, and all personal computers, laptops, notepads, and other electronic data processing equipment connected to any telephone line or network belonging to, or provided by, the City of Montgomery.

12.4.2 Email, Internet, and Intranet access (“Electronic Access”)
Electronic Access includes information technology but is not limited to: personal computers and related peripheral equipment and software, library resources, Internet/Intranet connectivity and access to Internet/Intranet services, and email.

12.4.3 Employee
Employee includes both City employees, and employees working under contract for the City that are provided electronic access by the City.

12.4.4 Employee Non-Work Time
Employee Non-Work Time means times when the employee is not otherwise expected, as determined by his/her Department Head, to be addressing official business, including off duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if the duty station and electronic access are normally available at such times). For employees working under contract for the City, Employee Non-Work Time includes time that is not billable to the City.

12.4.5 Information Technology
Information Technology means, for the purposes of this Policy/Procedure, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information.

12.4.6 Internet
The Internet is a global network connecting millions of computers. Unlike commercial online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer is independent. Its operators can choose which Internet services to use and which local services to make available to the global Internet community. Because there is no controlling or validating body for the information contained on the Internet, City employees are responsible for ensuring the accuracy and currency of any data downloaded from the Internet. The Internet is generally accessed using a web browser such as Internet Explorer.

12.4.7 Intranet
The Intranet is an internal network belonging to the City and is accessible only by City employees or others with authorization. An Intranet’s Web site looks and acts just like any other Internet Web site, but the firewall surrounding an Intranet fends off unauthorized access. The Intranet is generally accessed using a web browser such as Internet Explorer.

12.4.8 Mass Mailing
Mass Mailing is email sent to all or a majority of all members of more than one Department.

12.4.9 Minimal Additional Expense
Minimal Additional Expense means that the employee’s personal use of City electronic access is limited to those situations where the City is already providing electronic access or services for the employee’s work use. Examples of minimal additional expenses include, but are not limited to, using a computer printer to print out a few pages of material, infrequently sending personal email messages, or limited use of the Internet for personal reasons. Such use should incur only minimal additional expense to the City in areas such as:
* Communications infrastructure costs; e.g., telephone charges, telecommunications traffic, etc.
* Use of consumables in limited amounts, e.g., paper, ink, toner, etc.
* General wear and tear on equipment.
* Data storage on storage devices.
* Transmission impacts with moderate email message sizes such as emails with small attachments.

12.4.10 Personal Use
Personal Use means activity that is conducted for purposes other than accomplishing official or otherwise authorized City activities. However, this use must not violate any other City policy.

12.5 Procedures
12.5.1 Appropriate Usage
Appropriate use is always ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property and ownership of information; for security procedures; and for the individual's right to privacy and to freedom from harassment, intimidation, and unwarranted annoyance. Upholding safe computing standards and protecting the integrity of City computer resources is everybody’s responsibility. Every computer user must adopt operating behaviors that minimize opportunities for hackers or viruses to infiltrate the City.

The City maintains many databases that are considered For Official Use Only or Private. Employees may access this information and create files on their computers as necessary in the performance of their duties, but are responsible for providing appropriate protection.

12.5.1.1 Primary Usage
The primary usage of City-provided electronic access is for the accomplishment of City business. Appropriate business uses of City electronic access include, but are not limited to:
* Conducting official City business
* Collaborative work among various employees or Departments
* The delivery in electronic form of City services
* The dissemination of information about City activities and services
* The exchange of information and ideas among City employees, citizens, government agencies, community groups, and businesses.

12.5.1.2 Email Services
The City of Montgomery provides its employees with email services for the purpose of conducting City business. Typical acceptable uses of email include, but are not limited to:
* Sending and/or receiving official City correspondence to locations or addresses internal or external to the City.
* Mass mailings of official information throughout the City when the message is pertinent to the vast majority of the recipients, including:
  ** Job Announcements
  ** Meeting announcements
  ** Newsletters
  ** Service notices and schedules
  ** Staff Notices
  ** Correspondence and inquiries of a business nature with other City employees, vendors and suppliers
* Technical support
* Sharing documents or information as email attachments including product updates

12.5.1.3 Web Services
The City of Montgomery provides its employees with Web Services, including Internet and Intranet, for the purpose of conducting City business. Generally, web access should supplement the tools and information available to the employee, leading to an increase in the employee’s productivity or quality of work. The employee, and not the City, is responsible for checking copyright or licensing.
agreements before downloading and/or using information, files, or images from the Internet. Typical acceptable uses of Web Services include, but are not limited to:
* Accessing City information on the Internet or Intranet
* Catalogs (related to city business)
* Exchanging or requesting information with appropriate Web Sites
* Finding places and maps
* Form requests for permits or licenses
* Information requests for city requirements or regulations
* Locating product manuals
* New product research
* New research data
* On-line computer or professional training
* Ordering products for the City
* People and addresses
* Product fixes and upgrades
* Searching for helpful information of a business nature
* Technical support
* Other information related to city business

12.5.1.4 Limited Personal Use
Limited personal use of electronic access is also authorized, and each Department Head is responsible for establishing appropriate standards within his/her Department. Employees are allowed to use electronic access for non-City purposes when such use involves minimal additional expense to the City, is performed on the employee’s nonwork time, does not interfere with the mission or operations of the City, Department, or office, and does not violate any other Policy, law or regulation. Employees, however, have no inherent right to City electronic access, and such access is at the discretion of individual Department Heads. Additionally, information technology equipment availability and/or limitations may preclude an employee from having electronic access. Use of City electronic access for non-City purposes may be revoked or limited at any time by appropriate City Department Heads.

12.5.2 Inappropriate Usage
Employees are expected to conduct themselves professionally in the workplace and to refrain from using City electronic access for activities that are inappropriate. Misuse or inappropriate personal use of City electronic access includes, but is not limited to:
* Activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that is prohibited by nondiscrimination laws that are applicable to the City
* The creation, downloading, viewing, storing, copying, or transmission of sexually explicit or sexually oriented materials
* The creation, downloading, viewing, storing, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited
* Engaging in any outside fund raising activity or endorsing any product or service unless officially sanctioned and approved by the City.
* Engaging in any prohibited partisan political activity.
* Releasing City information to external news groups, bulletin boards or other public forums without City consent. This includes but is not limited to any use that could create the perception that the communication was made in one’s official capacity as a City employee unless appropriate City approval has been obtained, or uses contrary to the City’s mission or positions
* Any use that could generate more than minimal additional expense to the City
* The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data
* Maintaining or supporting a personal or private business, or support of “for-profit” activities or other outside employment or business activity. The ban on using City electronic access also includes employees using City electronic access to assist relatives, friends, or other persons in such activities
* Making or using illegal copies of copyrighted software, video, or music, storing such copies on City computers, or transmitting them over City communication channels
* Using unlicensed software, or using shareware beyond its evaluation period
* “Snooping” in another person’s email or files
* Trying to bypass or subvert the City’s security measures
* Supporting or soliciting support on behalf of groups not affiliated with the City unless officially sanctioned and approved by the City
* Downloading music or video, including streaming music or video, for non-City usage
* Any personal use that could cause congestion, delay, or disruption of service to any City system or equipment
* Using City systems to gain unauthorized access to other systems
* The creation, copying, transmission, or retransmission of chain letters or other unauthorized mailings regardless of the subject matter
* Mass mailings of:
  ** Any email when the message is not pertinent to the vast majority of the recipients
  ** Lost-and-found items
  ** Personal information, such as items “for sale”
  ** Routine address and telephone number changes
The restrictions on acceptable subject content apply to all aspects of the City’s resources. Obviously the policy applies to email and accessing Internet sites, but it also applies to files a user may create. The subjects listed above are unacceptable in any form, except as necessary for the Montgomery Police, Fire, and Legal Departments in the course of legal investigations.

12.5.3 Protection of Confidentiality Information
The information contained in or processed by City Computing Resources may be confidential and employees are responsible for preventing unauthorized disclosure or compromise of such information. Some (but not all) categories of confidential data include:
* Personal information such as Social Security numbers
* Procurement or contract sensitive information
* Health Insurance Portability and Accountability Act (HIPAA) information
* Client/Attorney Privilege and attorney work product information
Departments are responsible for incorporating proper procedures to prevent unauthorized disclosure or compromise of such information. The use of password protection or file permissions are generally accepted methods to safeguard confidential information by limiting access to the files to authorized individuals, and should be incorporated, as appropriate, to ensure information security. Employees and Departments must realize, however, that the tools necessary to manage the City Computing Resources allows employees of the Department of Information Technology to read these files even when such safeguards are taken. Encryption techniques should also be implemented, if necessary, to prevent even the Department of Information Technology from reading these files.

12.5.4 Reporting Violations
Employees observing violations, or receiving emails in violation of this Policy/Procedure, should report the violation as follows:
* Matters of a criminal nature should be reported to Montgomery Police Department
* Materials that violate nondiscrimination laws applicable to the City, including but not limited to sexual harassment, shall be reported following the guidelines specified in the “Montgomery Policy on Harassment in the Workplace” produced by the Personnel Department
* Violations that result in more than minimal additional expense to the City, misuse of City electronic access, and all other violations should be reported to the offending employee’s supervisor, Department Head, or equivalent.

12.5.5 Ownership and Monitoring
All software, computer files (including email), and data maintained or accessed using City resources are the property of the City. Licensed software and private data collected by the City should not be copied for use outside the workplace, destroyed without authorization, or otherwise misused. Violations of this sort may be illegal and lead to criminal prosecution. Users who violate copyright declarations are acting outside the course and scope of their employment and are personally responsible and liable for their actions. The City is relieved of any legal responsibility in such matters.

12.5.6 Privacy Expectations
Except as herein provided, the User, by acknowledging this Policy/Procedure understands and agrees that the City of Montgomery and its authorized representatives shall at all times have access to any information stored on, transmitted on, or viewed on any computer, personal digital assistant (PDA), or other City-owned resource. To the extent that employees wish that their private activities remain private, they should avoid using City Computing Resources even if that activity is otherwise authorized by this Policy/Procedure. Except as herein provided, by using City Computing Resources, City employees consent to disclosing to the City and its authorized representative the contents of any and all files or information maintained on or passed through City Computing Resources; and consent to monitoring and recording of their access to and use of electronic equipment that is covered by this Policy/Procedure with or without cause or prior notification. This Policy/Procedure and the acknowledgement of this Policy/Procedure do not affect, impair, modify, eliminate, or waive the responsibility to appropriately protect legal or confidential information; do not operate as a waiver of any attorney-client privilege; do not operate to waive or destroy any rights to keep information confidential under any work-product doctrine; and shall not operate to waive, destroy, impair, or absolve the rights or obligations of the City of Montgomery or its officers or agents to keep information confidential. While some business units may be using security measures that ensure confidentiality of information, the general understanding is that such use is not secure, is not private, and is not anonymous. System managers do occasionally employ monitoring tools to detect improper use and perform remote hardware and software auditing. Electronic communications may be disclosed within the City or Department to employees who have a need to know in the performance of their duties.

12.5.7 Sanctions for Misuse
Unauthorized or improper use of City Computing Resources could result in loss of job, limitations on the use of City Computing Resources, disciplinary or other adverse actions, criminal penalties, and/or employees being held financially liable for the cost of improper use.

12.5.8 Responsibilities
12.5.8.1 Employee
Access to the City’s Computing Resources is a privilege, not a right. Violation of any portion of this policy may result in the cancellation of that privilege and in possible disciplinary action. Each employee’s primary responsibility, therefore, is to uphold all provisions of this policy. Every employee is responsible for his/her own actions and for actions conducted by any person who accesses the City’s resources using his/her access accounts or passwords. Good judgment and safe computing procedures should be exercised at all times. The employee is responsible for:
* Acknowledging acceptance and understanding of this Policy/Procedure by signing the “Request for City Computing Resources and User Acknowledgement of City Policy” at the end of this Policy / Procedure, and returning the signed form to the Department of Information Technology
* Following the directives of this Policy/Procedure
* Reporting violations of this Policy/Procedure following the guidelines in paragraph 12.5.4
* Safeguarding City data, including user accounts and passwords
* Ensuring he/she is not giving the false impression that he/she is acting in an official City capacity when using City electronic access for non-City purposes
* Ensuring the accuracy and currency of any data downloaded from the Internet
* Checking copyright or licensing agreements before downloading and/or using information, files, or images from the Internet, and are personally responsible and liable for their actions

12.5.8.2 Department of Information Technology
The Department of Information Technology is responsible for:
* Acting as the Mayor’s agent for this Policy/Procedure
* Providing a designee for the Legal Department as agent for this Policy/Procedure and to preserve and protect those confidential rights and privileges as set out in section 12.5.6
* Creating and maintaining this Policy/Procedure
* Reporting violations of this Policy/Procedure following the guidelines in paragraph 12.5.4
* Assisting City officials in investigating formally reported violations of this Policy/Procedure
* Maintaining the record of employees approved for access to City Computing Resources
* Safeguarding City resources by removing access to City Computing Resources for employees that depart the City or as otherwise requested by a Department Head

12.5.8.3 Department Heads
Are responsible for:
* Disseminating and enforcing this Policy, and monitoring employees for compliance with this Policy/Procedure
* Requesting and approving employee requests for access to City Computing Resources by co-signing the “Request for City Computing Resources and User Acknowledgement of City Policy” form at the end of this Policy/Procedure, and returning the completed form to the Department of Information Technology
* Notifying the Department of Information Technology when an employee departs the Department or City, or no longer requires access to City Computing Resources
* Reporting violations of this Policy/Procedure following the guidelines in paragraph 12.5.4
* Ensuring only approved employees access City Computing Resources
* Establishing appropriate standards within his/her Department for Limited Personal Use
* Assisting City officials in investigating violations of this Policy/Procedure
* Investigating violations of this Policy/Procedure by employees, including contractor employees, within their Department
* Applying appropriate discipline for misuse of City Computing Resources or violation of this policy in consultation with the Personnel Department

12.5.9 Request for City Computing Resources and User Acknowledgement of City Policy

12.5.9.1 Department Head Request
I, as Department Head, certify the following City employee has a valid need to access City Computing Resources. I further certify the City employee has read and understands the City of Montgomery’s “Policy/Procedure 06-011: Acceptable Use of City Computing Resources.” I further agree to notify the Department of Information Technology when this employee departs the Department or City, or no longer requires access to City Computing Resources.

12.5.9.2 Employee Acknowledgement
I, as a City of Montgomery employee, have read and understand the City of Montgomery’s “Policy/Procedure 06-011: Acceptable Use of City Computing Resources.” With my signature below, I agree to abide by this Policy/Procedure when using the City’s Computing Resources. I further agree to report any known or suspected violations of this Policy/Procedure following the procedures specified in this Policy/Procedure. I understand that the City may restrict or revoke my computer access privileges at any time without notice. I also acknowledge that my rights to privacy are limited as further described in paragraph 12.5.6 (Privacy Expectations).
16.3 Definitions
16.3.1 Absent Without Leave (AWOL)
An employee will be considered Absent Without Leave (AWOL) if he/she (1) is absent from his/her work location during any part of his/her scheduled shift without prior approved leave, (2) does not notify his/her supervisor that he/she will be absent, or (3) fails to respond to an emergency in accordance with “Policy/Procedure 06-005: Emergency Response”.

16.3.2 Applications Team Lead
The Applications Team Lead is the person responsible for managing the internal Department of Information Technology created software and vendor-supplied software applications and supporting products for the City of Montgomery.

16.3.3 AS/400
“The [IBM] AS/400—formally renamed the “IBM iSeries,” but still commonly known as AS/400—is a midrange server designed for small businesses and departments in large enterprises and now redesigned so that it will work well in distributed networks with Web applications. The AS/400 uses the PowerPC microprocessor with its reduced instruction set computer technology. Its operating system is called the OS/400.”

16.3.4 Authorized Software
Authorized Software is legally licensed software on City computers necessary for the accomplishment of City business, and includes Departmental-Unique Software, Productivity Software, Single Purpose Software, and Standard Software. Other types of software such as utilities or browser enhancements may be authorized provided the software is legally licensed and does not conflict with any other computer program or resources. The Department of Information Technology does not support all authorized software.

16.3.5 Authorized Vehicle Driver
An Authorized Vehicle Driver is a person (1) legally licensed to drive and (2) recognized by the Risk Department as an approved driver of City-owned Vehicles.

16.3.6 AWOL
See Absent Without Leave (AWOL).

16.3.7 Back-up On-Call Technician
The Back-up On-Call Technician is the Primary On-Call Technician’s Team Lead.

16.3.8 Back-up Team Lead
The Back-up Team Lead is the Department of Information Technology staff member assigned as the Team Leads of the Primary On-Call Technician. When the Primary On-Call Technician is not reachable, the Back-up Team Lead is responsible for handling customer service calls outside of regular business hours.

16.3.9 Casual Day
Casual Day is a workday where a more relaxed dress code is accepted. Employees must, even on Casual Day, portray an acceptable level of business professionalism. Within the City of Montgomery, past practice has established Friday as the usual day where casual dress is allowed, as permitted and specified by the Director or other City policy.

16.3.10 City Computing Resources
For the purpose of this policy, City Computing Resources include the City’s computer network, Internet, Intranet, and all personal computers, laptops, notepads, and other electronic data processing equipment connected to any telephone line or network belonging to, or provided by, the City of Montgomery.

16.3.11 City-related Business
City-related Business means Vehicle usage necessary for the accomplishment of City or Department of Information Technology business, to include travel to and from business locations, or other uses as may be authorized in advance by the Mayor or Executive Assistant to the Mayor.

16.3.12 Compensatory Time
Compensatory Time refers to a type of work schedule arrangement that allows workers to take time off instead of receiving Overtime pay.

16.3.13 Custom Software
According to the Attorney General (94-00023), Custom Software is “Software that will require substantial creative work by a professional/vendor to comply with unique specifications could constitute “custom software” within the meaning of Section 41-61-51(a)(11), Code.” For the purposes of this Procedure, custom software includes commercial software such as operating systems, network operating systems, database, and financial software.

16.3.14 Customer Support Coordinators
The Customer Support Coordinators are the Department of Information Technology team members responsible for handling customer issues and support citywide.

16.3.15 Customer Support Office
The Customer Support Office is the backup triage support location for the Help Desk when the Customer Support Coordinators are absent or otherwise busy. This office is also the staging area for configuring desktop equipment.

16.3.16 Customer Support Operations
The Customer Support Operations are the integral parts of the IT Triage Process.

16.3.17 Customer Support Team Lead
The Customer Support Team Lead is responsible for managing the Customer Support Operations and maintaining the rotation lists for staffing the Help Desk and the after duty day support by the Primary On-Call Technician. In an emergency, the Customer Support Team Lead will perform the duty defined in “Policy/Procedure 06-005: Emergency Response” (page 13).

16.3.18 Customer Support Technician
The Customer Support Technician is the individual(s) assigned to support the Help Desk. The Customer Support Technician works in the Customer Support Office.

16.3.19 Departmental-Unique Software
Departmental-Unique Software is legally licensed software generally installed on a small subset of the computers purchased by the City, typically to meet the business needs of a small number of employees or office(s). The Department of Information Technology may install Departmental-Unique Software, or this software may be installed by the individual Department in coordination with the Department of Information Technology. Support for Departmental-Unique Software is generally supplied by the installing Department. Examples of Departmental-Unique Software include, but are not limited to:
* Crime Index
* Financial
* Payroll
* Records Management System
* Selected GIS applications

16.3.20 Dress Shirt
The Dress Shirt is a collared shirt with buttons as described in paragraph 15.5.2.

16.3.21 Email, Internet, and Intranet access (“Electronic Access”)
Electronic Access includes information technology but is not limited to: personal computers and related peripheral equipment and software, library resources, Internet/Intranet connectivity and access to Internet/Intranet services, and email.

16.3.22 Emergency
An Emergency is a situation that poses an immediate threat to human life or serious damage to property.

16.3.23 Emergency Operations Center (EOC)
The Emergency Operations Center (EOC) is within the City Communications facility located at 911 Communications Parkway, Montgomery, AL. Also housed within this facility are the Emergency Management Agency (EMA) offices and the 911 Communications Center.

16.3.24 Employee
Employee includes both fulltime and part-time City employees, and employees working under contract for the City.

16.3.25 Employee Non-Work Time
Employee Non-Work Time means times when the employee is not otherwise expected, as determined by his/her Department Head, to be addressing official business, including off duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if the duty station and electronic access are normally available at such times). For employees working under contract for the City, Employee Non-Work Time includes time that is not billable to the City.

16.3.26 Engineering Services
Engineering services are the work products of computer engineers involving the design, construction, and operation of computer systems. Computer engineers work on both computer hardware and software (programming) problems. Engineering services is also known as Professional Services.

16.3.27 Excused Absence or Tardiness
An Excused Absence or Tardiness is an Unscheduled Absence or Tardiness for which the Director feels an extenuating circumstance exists which precluded the employee from providing advance notice.

16.3.28 Family Medical Leave Act (FMLA)
The Family Medical Leave Act (FMLA) is a federal law administered by the Personnel Department that requires employers to provide an employee with 12 weeks of unpaid leave during a year’s time for the birth or adoption of a child, family health needs, or personal illness. The employer must allow the employee to return to the same position or a position similar to that held before taking the leave.

16.3.29 Fleetwatch
Fleetwatch is a Montgomery Police Department program intended to reduce crime by extending the eyes and ears of the Police Department. This program uses other City employees to observe suspicious activities and report it. Since your work may take you into residential and business neighborhoods, you are in a position to see activity nor normally seen by the Police. Questions about the Fleetwatch program should be referred to the MPD Community Policing Division at (334) 240-4800.

16.3.30 Help Desk
The Help Desk is the centralized location for receiving and documenting support request calls from customers.

16.3.31 Incidental Equipment Purchase
An Incidental Equipment Purchase is (1) the purchase of any equipment under a contract whose specified intent does not include hardware, (2) is directly related to the contract purpose and necessary for the completion of this contract service, and (3) is of a value of minor proportions to the overall contract price or represents a minor portion of the work to be accomplished.

16.3.32 Information Technology
Information Technology means, for the purposes of this Policy/Procedure, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information.

16.3.33 Internet
The Internet is a global network connecting millions of computers. Unlike commercial online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer is independent. Its operators can choose which Internet services to use and which local services to make available to the global Internet community. Because there is no controlling or validating body for the information contained on the Internet, City employees are responsible for ensuring the accuracy and currency of any data downloaded from the Internet. The Internet is generally accessed using a web browser such as Internet Explorer.

16.3.34 Intranet
The Intranet is an internal network belonging to the City and is accessible only by City employees or others with authorization. An Intranet’s Web site looks and acts just like any other Internet Web site, but the firewall surrounding an Intranet fends off unauthorized access. The Intranet is generally accessed using a web browser such as Internet Explorer.

16.3.35 Legally Licensed Software
Legally Licensed Software is software that is acquired, installed, maintained, and used in accordance with the manufacturer’s software license.

16.3.36 Level 1 Support
Level 1 Support occurs when the Customer Support Technician works Service Request while at the Help Desk. This is accomplished when the Customer Support Technician handles the request/problem over the telephone by instructing the user or by using Remote Desktop Tools.

16.3.37 Level 2 Support
Level 2 Support is the support conducted at the requester’s or user’s location. The Customer Support Technician is required to make an appointment, travel to the users’ location, provide onsite support, and document the results/resolution in the Work Order System.

16.3.38 Level 3 Support
Level 3 Support is the escalated level of support requiring expert assistance in dealing with the service request. The expert assistance is provided by senior level management staff/Teams or contractor personnel.

16.3.39 Mass Mailing
Mass Mailing is email sent to all or a majority of all members of more than one Department.

16.3.40 Minimal Additional Expense
Minimal Additional Expense means that the employee’s personal use of City electronic access is limited to those situations where the City is already providing electronic access or services for the employee’s work use. Examples of minimal additional expenses include, but are not limited to, using a computer printer to print out a few pages of material, infrequently sending personal email messages, or limited use of the Internet for personal reasons. Such use should incur only minimal additional expense to the City in areas such as:
* Communications infrastructure costs; e.g., telephone charges, telecommunications traffic, etc
* Use of consumables in limited amounts, e.g., paper, ink, toner, etc
* General wear and tear on equipment
* Data storage on storage devices
* Transmission impacts with moderate email message sizes such as emails with small attachments

16.3.41 Network Team Lead
The Network Team Lead is the person responsible for monitoring, controlling, and supporting the citywide network infrastructure (wired and wireless).

16.3.42 Operations Team Lead
The Operations Team Lead is the person responsible for managing the server and backroom operations in various locations around the City of Montgomery.

16.3.43 Overtime
Overtime is time worked beyond the employee’s established work limit and generally results in additional payment.

16.3.44 Personal Use
Personal Use means activity that is conducted for purposes other than accomplishing official or otherwise authorized City activities.

16.3.45 Policy
A Policy is a guiding principle used to set direction in an organization. It can be a course of action to guide and influence decisions. It should be used as a guide to decision making under a given set of circumstances within the framework of objectives, goals, and management philosophies as determined by senior management.

16.3.46 Primary On-Call Technician
The Primary On-Call Technician is the rotating Department of Information Technology staff member assigned the responsibility for handling customer service calls outside of regular business hours. In an emergency, the Primary On-Call Technician performs the duty defined in “Policy/Procedure 06-005: Emergency Response” (page 13).

16.3.47 Procedure
A Procedure is a particular way of accomplishing something. It should be designed as a series of steps to be followed as a consistent and repetitive approach or cycle to accomplish an end result. Procedures provide a platform for implementing the consistency needed to decrease process variation, which increases procedure control. Decreasing process variation is one way to eliminate waste and increase performance.

16.3.48 Productivity Software
Productivity Software is approved enabling software technology that allows employees to perform their assigned tasks. Departmental-Unique Software and Standard Software are examples of Productivity Software.

16.3.49 Proof of Medical Treatment
Proof of Medical Treatment is written and signed documentation from a medical doctor stating the employee has been under the doctor’s treatment for a medical condition that has resulted in the employee’s absence or tardiness. The Proof of Medical Treatment does not need to include a diagnosis or cause for treatment, but must state the timeframe that is covered.

16.3.50 Remote Desktop Tools
Remote Desktop Tools are programs that allow a Customer Support Technician to connect to another person's computer via the network and perform all actions as though physically in contact with the computer. A Customer Support Technician can view remotely from his/her work location the contents of a user's PC at the user's location and execute actions to resolve requests/problems.

16.3.51 Requests for Reimbursement

Requests for Reimbursement are an employee’s request for Compensatory Time or Overtime submitted on a Leave/Overtime Request Form.

16.3.52 Scheduled Absence

A Scheduled Absence is any absence, tardiness, or early departure from work that has been scheduled by the employee in advance in accordance with paragraph 3.5.6.1. Within the Department of Information Technology, an absence will be considered a Scheduled Absence if (1) the absence has been approved before the beginning of the requested leave period and (2) a minimum of two working days advance notice is given.

16.3.53 Senior City Staff Member

Senior City Staff Members include the Mayor, Executive Assistants to the Mayor, and Department Directors.

16.3.54 Service Level Agreement

Service Level Agreements are agreements between the customers of IT service and the Department of Information Technology for the degree of support that IT is expected to provide under various circumstances.

16.3.55 Service Request

A Service Request is the documented summary of a user’s request, which is maintained in the Work Order System. The terms “Service Request” and “Work Order” are interchangeable.

16.3.56 Service Vehicle

A Service Vehicle is any Vehicle assigned to the Department of Information Technology other than any Vehicle permanently assigned to the Director or Assistant Director.

16.3.57 Single Purpose Software

Single Purpose Software is software performing basically a dedicated and unique service or function, such as radio frequency control software, E911 software, or parking deck software, and is not considered Productivity Software or Departmental-Unique Software. Typically, Single Purpose Software is run on a computer system dedicated solely for this function and no other function. Support for Single Purpose Software is generally provided by the using Department, frequently under contract from the manufacturer.

16.3.58 Software License

A Software License is a legal contract outlining the terms and conditions of how an individual, group, or company may install and/or use a particular piece of software. Most software is licensed in some fashion, even if the software is free. The license typically includes the number of computers that may use the software (frequently limited to one computer unless additional fees are paid); the type and cost of manufacturer support; how long the software may be used without paying additional fees; etc. The City, Departments, and/or individual employees may be held liable for violation(s) of applicable software licenses. Possession of a valid or legal compact disk (CD) containing the software does not automatically grant permission to use the software. Additionally, software downloaded without any charge from the Internet does not automatically mean that the software is either free, installable on any machine, or has unlimited usage. Downloaded software has a license that must be honored, including payment of any applicable fees.

16.3.59 Sponsoring Department

The Sponsoring Department is the City of Montgomery Department requesting creation of a VPN.

16.3.60 Standard Software

Standard Software is legally licensed and supported software generally installed on most City computers. The Department of Information Technology usually installs Standard Software. Examples of standard software include, but are not limited to:

* Adobe Reader
* Java
* Microsoft Internet Explorer
* Microsoft Office (Word, Excel, Outlook)
* Microsoft Windows
* Windows Media Player
16.3.61 Supported Software
Supported Software is the inventory of legally licensed software for which the Department of Information Technology can provide technical assistance. In general, Supported Software is software used on the majority of City computers. Standard Software and some Departmental-Unique Software are examples of supported software. As newer versions of Supported Software are released, support for older versions will eventually be curtailed. Single Purpose Software is generally not Supported Software.

16.3.62 Team Function Lists
The Team Function Lists are the documented allocations of staff responsibilities for products and functions, which the Department of Information Technology provides to users/customers of the City of Montgomery’s computer-network services. The Team Function Lists are grouped according to the Department of Information Technology’s four integrated teams.

16.3.63 Team Leads
The Department of Information Technology is organized around four integrated Teams, each with its own leader. The Team Leads are Applications Team Lead, Customer Support Team Lead, Network Team Lead, and Operations Team Lead.

16.3.64 Teams
The Department of Information Technology is organized around four integrated Teams: Applications, Customer Support, Network, and Operations.

16.3.65 Triage Process
The Triage Process is a methodology of handling the worst, most demanding problems first. These problems are given the highest priority because they can cause serious impacts to the organization. Customer Support Technicians sort through incoming service requests to identify the Urgent Priority requests. The Work Order System prompts the Customer Support Technician when existing service requests become Urgent Priority due to missed due dates and not meeting Service Level Agreement with IT customers.

16.3.66 Unauthorized Software
Unauthorized Software is any software that is not installed by, or in coordination with, the Department of Information Technology; not legally licensed; does not contribute to official City business needs; poses a security risk; impacts network performance; uses excessive computing resources; not authorized Single Purpose Software; individually or personally purchased software, whether legally licensed or not; or is otherwise not approved by the Department of Information Technology. Examples of unauthorized software include, but are not limited to:

* Flight simulators
* Gambling (whether for fun or profit)
* Games
* Music downloads
* Napster
* Peer-to-peer file sharing
* Tax software
* VPN (Virtual Private Network) software not installed and configured by the Department of Information Technology

16.3.67 Unexcused Absence or Tardiness
An Unexcused Absence or Tardiness is an Unscheduled Absence or Tardiness for which the Director feels an extenuating circumstance does not exist which precluded the employee from providing advance notice.

16.3.68 Uniform
A Uniform is a “distinctive outfit intended to identify those who wear it as members of a specific group.”6 Within the Department of Information Technology, a Uniform shall consist of a collared shirt or blouse as prescribed by the Director.

16.3.69 Unscheduled Absence or Tardiness
An Unscheduled Absence or Tardiness is any absence, tardiness, or early departure of any time duration not in accordance with paragraph 3.5.6.1 and reported in accordance with paragraph 3.5.6.2.

16.3.70 Unsupported Software
Unsupported Software is unauthorized software or any software that does not fit the definition of “Supported Software.” Unsupported software is not eligible to receive any technical support from the Department of Information Technology and, if determined to cause a conflict with other software, will be
removed by the Department of Information Technology. Examples of unsupported software include, but are not limited to:
* AOL software
* E-mail clients other than Microsoft Outlook
* Firefox
* Google, MSN, Yahoo, or other toolbar extensions
* Instant messaging
* Netscape
* OpenOffice
* Yahoo Toolbar

16.3.71 Urgent Priority
An Urgent Priority is a Work Order System classification for service requests involving a work stoppage or a significant system outage.

16.3.72 Vehicle
For the purposes of this Policy, a Vehicle is any automobile, van, minivan, sport utility vehicle (SUV), pick-up, or truck owned or provided by the City of Montgomery.

16.3.73 Vehicle Custodian
The Vehicle Custodian is the Department of Information Technology person assigned the duty of monitoring and tracking all Departmental Vehicles usage and maintenance.

16.3.74 Vehicle Usage Log
The Vehicle Usage Log is the Department of Information Technology document used to track the usage of Departmental Vehicles.

16.3.75 VIP Priority
A VIP Priority is a Work Order System classification for service requests involving a Senior City Staff Member.

16.3.76 Virtual Private Network
A Virtual Private Network “is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization’s network... A VPN works by using the shared public infrastructure while maintaining privacy through security procedures...”7 Since a VPN uses a public infrastructure, extra precautions must be taken to safeguard security.

16.3.77 VPN
See Virtual Private Network.

16.3.78 Weekly Work Order Meeting
The purpose of the Weekly Work Order Meeting is to review, evaluate, and prioritize open Service Request.

16.3.79 Work Order
See “Service Request.”

16.3.80 Work Order System
The Work Order System is the computerized retention, processing, and reporting of Service Request. The Service Request are updated through status changes and date stamps, and tracked throughout their lifecycles. A Customer Support Technician is prompted when a Service Request is overdue or a Service Level Agreement is breached.

16.3.81 Work Shirt
The Work Shirt is a polo-style shirt as described in paragraph 15.5.2.
Emergency Response
6.1 Purpose
The purpose of this Policy and Procedure is to document emergency response expectations and duties for personnel within the Department of Information Technology.

6.2 Policy
It is the policy of the Department of Information Technology to support the City's response to an emergency on a 24x7 basis.

6.3 Applicability
This Policy and Procedure is applicable to all Department of Information Technology employees.

6.5 Procedures
6.5.1 Declaration of Emergency
The Mayor of the City of Montgomery or the Director of the Emergency Management Agency (EMA) may declare an emergency for the region resulting in the automatic activation of these procedures. Additionally, the Department of Information Technology Director may invoke these procedures, when needed, even if an emergency has not been declared by the Mayor or EMA Director.

6.5.2 Departmental Staff Actions
All staff members will respond as tasked to an emergency on a 24x7 basis. These duties take precedence over any other duties for the duration of the emergency. Staff members recalled to work will be prepared to remain at work until relieved by another Department of Information Technology staff member or officially released by the Department of Information Technology Director, Assistant Director, or EMA official. Staff members not immediately recalled to work will be prepared to serve scheduled rotational duties or other functions as directed. This Policy/Procedure attempts to address the roles and responsibilities of Department of Information Technology staff members in an emergency or disaster, but cannot document each and every situation or variation. Staff members are expected to adjust these plans according to the actual situation following guidance given by senior City officials and using their best judgment. Immediate actions are critical to the success of the emergency response. Staff members need to understand that, during an emergency, you have a great deal of responsibility and authority. Be prepared to exercise both of those in the best interests of the City and the Department of Information Technology.

6.5.2.1 Director
The Department of Information Technology Director will be notified by appropriate City staff that an emergency has been declared. In the absence of the Director, the Assistant Director will fulfill this role. Upon notification, he/she will:
1. Ensure Department of Information Technology emergency procedures are invoked and followed.
2. Notify and provide recall instructions to:
   2.1. Assistant Director
   2.2. Applications Team Lead
   2.3. Customer Support Team Lead
3. Immediately report to the Emergency Operations Center (EOC), and remain at the EOC until replaced by another Department of Information Technology staff member or until the emergency is over.
4. Serve as the focal point to coordinate and resolve any EOC information technology needs, issues, and/or problems.
5. Assist the Mayor, EMA Director or Assistant Director, and other City/County officials, as needed.

6.5.2.2 Assistant Director
Upon notification, he/she will:
1. In the absence of the Director, fulfill the role of the Director as described in paragraph 6.5.2.1 above.
2. Notify and provide recall instructions to:
   2.1. Network Team Lead
   2.2. Operations Team Lead
3. Immediately report to City Hall, and remain at the City Hall until replaced by another Department of Information Technology staff member or until released by the Director.
4. Safeguard and protect all Department of Information Technology IT resources.
5. Coordinate all IT support issues between the Emergency Operations Center (EOC) and City Hall.
6. Recall other Department of Information Technology staff, as necessary. For a prolonged emergency, establish a rotation schedule for all Department of Information Technology employees to ensure continued 24x7 emergency support coverage.

6.5.2.3 Applications Team Lead
Upon notification, he/she will:
1. Immediately report to the Emergency Operations Center (EOC), and remain at the EOC until replaced by another Department of Information Technology staff member or until released by the Department of Information Technology Director.
2. Ensure EOC IT equipment is operational, and remains operational throughout the emergency.
3. Assist EOC staff with IT related issues.

6.5.2.4 Customer Support Team Lead
Upon notification, he/she will:
1. Immediately log into the City of Montgomery IT system via VPN.
2. Remain in contact with the Director and/or Applications Team Lead to determine any support requirements needed.
3. Be prepared to report to the Emergency Operations Center (EOC) if directed.
4. Ensure IT equipment is operational, and remains operational throughout the emergency.
5. Assist with IT related issues.

6.5.2.5 Network Team Lead
Upon notification, he/she will:
1. In the absence of the Assistant Director, fulfill the role of the Assistant Director as described in paragraph 6.5.2.2 above.
2. Immediately report to City Hall, and remain at the City Hall until replaced by another Department of Information Technology staff member or until released by the Director or Assistant Director.
3. Ensure City Hall equipment is operational, and remains operational throughout the emergency.

6.5.2.6 Operations Team Lead
Upon notification, he/she will:
1. Immediately log into the City of Montgomery IT system via VPN.
2. Remain in contact with the Assistant Director and/or Network Team Lead to determine any support requirements needed.
3. Be prepared to report to the City Hall if directed.
4. Ensure IT equipment is operational, and remains operational throughout the emergency.
5. Assist with IT related issues.

6.5.2.7 Other Departmental Staff
Other Department of Information Technology staff members not otherwise specified in this Policy/Procedure may be required to assist during an emergency as directed by the Director or Assistant Director.

6.5.3 General Guidelines
6.5.3.1 Safety
Safety is paramount, and you should not attempt any action that will jeopardize your safety.

6.5.3.2 Respond in a Timely Fashion
As with any emergency, time is of the essence. Employees should be prepared to respond in a timely fashion using whatever transportation means available if, and when, the need arises. This includes the possibility of responding outside of normal duty hours as the emergency may preclude following normal work schedules.

6.5.3.3 Uniform Wear
When responding to an emergency, Uniform wear is optional if time does not allow.

6.5.3.4 Failure to Respond
Failure to respond in a timely fashion could result in the employee being considered Absent Without Leave (AWOL) (see paragraph 3.5.7.1). An employee will not be considered AWOL if the employee failed to respond to an Emergency if the employee felt it was unsafe (paragraph 6.5.3.1).
Help Desk
8.1 Purpose
The purpose of this Policy and Procedure is to define the operations for the Department of Information Technology Help Desk.
8.2 Policy
It is the Policy of the Department of Information Technology to support City information technology customers in a timely fashion.
8.3 Applicability
This Procedure is applicable to all Department of Information Technology employees.
8.5.1 Emergency Response
When notified of an emergency, Departmental staff will perform alternate duties as described in “Policy/Procedure 06-005: Emergency Response” (page 13). These duties take precedence over any other duties specified in this Policy/Procedure for the duration of the emergency.
8.5.2 Service Requests
Customers contact the Department of Information Technology by calling 5555 or via email.
8.5.3 Customer Support Team Lead
8.5.3.1 Establish Rotation Schedules
The Customer Support Team Lead will establish and publish the rotating work schedules for the Customer Support Coordinators, Primary On-Call Technician, and Back-up Team Lead.
8.5.3.2 Training
The Customer Support Team Lead is responsible for ensuring appropriate staff is trained in the procedures to Handle Customer Service Requests.
8.5.3.3 Weekly Work Order Meeting
The Customer Support Team Lead will:
1. Be the person in charge of the Weekly Work Order Meeting.
2. Ensure:
   2.1. The Meeting is conducted.
   2.2. Service Request(s) are assigned per priorities.
   3. Conduct a review of the Service Request, looking for:
      3.1. New Service Requests that need evaluation and assignment.
      3.2. Service Request(s) that were not handled following “Policy/Procedure 06-003: Scheduling Customer Appointments.”
      3.3. Service Request excessively long.
      3.4. Repeat or problematic issues are identified.
      3.5. Service Request(s) requiring additional technical expertise or assistance.
      3.6. Service Request(s) that have been completed but not marked as closed by the responsible Technician.
4. Reassign existing Service Request, as appropriate.
5. Inform the Director of any work order:
   5.1. Requiring management involvement.
   5.2. Open excessively long.
   5.3. Repeat or problematic issues.
6. Ensure the Work Order System is updated to reflect all changes.
7. Produce a Weekly Recap to be presented at the next Departmental Staff Meeting summarizing:
   7.1. Urgent Priority Service Requests handled in accordance with paragraph 8.5.4.1.3.2.
   7.2. Service Request(s) involving a Senior City Staff Member.
   7.3. Calls handled outside of normal business hours.
   7.4. Calls handled without dispatching a Technician (per paragraph 8.5.4.1.2).
   7.5. Service Request(s) that were not handled following “Policy/Procedure 06-003: Scheduling Customer Appointments.”
7.6. Service Request(s) open excessively long.
7.7. Repeat or problematic issues are identified.
7.8. Other metrics as appropriate to quantify the Department of Information Technology workload.

8.5.4 Customer Support Coordinators
The Customer Support Coordinators’ responsibilities include:
8.5.4.1 Handle Customer Service Requests
The Customer Support Coordinators will be responsible for calls received on extension 5555.

8.5.4.1.1 Answer Calls
1. The Customer Support Coordinators are the primary staff responsible for:
   1.1. Answering and handling the telephone.
   1.2. Recording the Service Request in the Work Order System (per paragraph 8.5.4.1.2).
   1.3. When needed, routing the call to an escalation level staff member.
2. If the call is not answered by one of the Customer Support Coordinators, the telephone call will automatically be routed to the Customer Support Office to be handled by an alternate Technician.
3. If the call is not answered by the alternate Technician, the telephone call will automatically be routed to the Office Manager to be handled.

8.5.4.1.2 Document Service Requests
All Service Requests, including those not requiring a Customer Support Technician to be dispatched, will be recorded in the Work Order System and will include, at a minimum:
1. The date and time of the Service Request
2. The name, department, contact information, and location of the person requesting service
3. The reason for the Service Request
4. The priority or urgency of the Service Request
5. The status of the Service Request, and
6. Resolution or solution, if provided

8.5.4.1.3 Service Request Handling and Routing
The Customer Support Coordinators will perform the initial triage for all Service Requests.

8.5.4.1.3.1 Requests Involving a Senior City Staff Member
For Service Requests involving a VIP/Senior City Staff Member, the Customer Support Coordinators will immediately:
1. Record the Service Request as a “VIP Priority.” The Work Order System will automatically notify the Director and Assistant Director regarding the details of this Service Request.
2. If specified by the Director or Assistant Director, take the actions to work the request as soon as possible.

8.5.4.1.3.2 Urgent Priority Service Requests
For Service Requests that are Urgent Priority, the Customer Support Coordinators will immediately notify the Team Leads and the Director or Assistant Director for direction and:
1. Record the Service Request as an “Urgent” priority Work Order. The Work Order System will automatically report the status of the Service Request to the Director and Assistant Director. The Customer Support Coordinators will also notify the Customer Support Team and other applicable technicians.
2. If specified by the Director or Assistant Director, notify City users impacted by an outage.
3. Will maintain awareness of the status of the work order until it is completed. Team Leads will take the actions to immediately work the request and complete it and, if necessary, reassign other Department of Information Technology staff members and reschedule other Service Requests to complete the work as immediately as possible.

8.5.4.1.3.3 Other Service Requests
For all other Service Requests, the Customer Support Coordinators:
1. For Level 1 Support, handles the request over the telephone during the initial customer contact.
2. For Level 2 Support:
   2.1. Determines which IT staff member should be assigned, following the guidance in the Team Function Lists.
   2.2. Updates the Work Order System to reflect this assignment. The Work Order System will automatically notify the assigned staff member.
3. For non-technical questions or requests beyond the knowledge of the Customer Support Coordinators, transfers the request to the appropriate IT staff member following the guidance in the Team Function Lists.

8.5.4.2 Work Order System Improvements
The Customer Support Team Lead is also designated the Department of Information Technology “owner” of the Work Order System. As such, he/she shall continuously review the Work Order System for possible improvements in record tracking and reporting, including the introduction of tracking Library, Communications Department IT-related tasks, and AS/400 items. Such improvements will be discussed with the Director before implementation.

8.5.5 Customer Support Technician
The Customer Support Technician is responsible for:
1. At the beginning of each workday, reviewing outstanding work orders assigned to him/her to plan the execution of Work Orders to:
   1.1. Make appropriate arrangements to complete Work Orders in the assigned timeframe including scheduling service calls per “Policy/Procedure 06-003: Scheduling Customer Appointments.”
   1.2. Notify his/her Team Leads, along with rationale, if the Work Order cannot be completed in the assigned timeframe.
2. Updating the content and status of Work Orders assigned to him/her no later than the close of business each workday.
Scheduling Customer Appointments
4.1 Purpose
The purpose of this Policy and Procedure is to document scheduled customer appointment expectations and procedures within the Department of Information Technology.
4.2 Policy
As a courtesy to City employees and to ensure efficient Departmental operations, all Department of Information Technology staff members should attempt to schedule a mutually convenient time with the customer to perform troubleshooting and service repairs onsite at the customer’s location or offsite by Remote Desktop Tools.
4.3 Applicability
This Policy and Procedure is applicable to all Department of Information Technology employees.
4.5 Exceptions to Policy
This Policy recognizes that it may not be possible, or is impractical, to attempt to schedule an appointment for every Service Request and allows for the judgment of individual Customer Support Technicians in this regard. The following are examples of acceptable exceptions to this policy:
1. An emergency per “Policy/Procedure 06-005: Emergency Response.”
2. Urgent Priority requests involving major system outages per the IT Triage Process;
3. Urgent issues involving a Senior City Staff Member (referred to as “VIP Priority” in the Work Order System);
4. Issues that are highly time sensitive, such as a failure during an important City meeting or event;
5. “Trivial” requests that can be resolved in a matter of minutes over the telephone or with Remote Desktop Tools by a Customer Support Technician (Level 1 Support);
6. Special arrangements as directed by one of the Team Leads. If there is a question about whether an Exception should be applied, contact the Director or Assistant Director for an interpretation.
4.6 Procedures
1. Before attempting service on a Service Request onsite at the customer’s location or offsite through Remote Desktop Tools, the Customer Support Technician will:
   1.1. Contact the customer to establish a mutually convenient time for the service.
   1.2. Record the appointment in the Work Order System.
   1.3. Invite the customer in his/her Microsoft Outlook Calendar with a reminder that will prompt the Customer Support Technician before the appointment.
2. If the customer cannot be contacted, the Customer Support Technician will leave a call-back message for the customer.
3. If the Customer Support Technician discovers that he/she will not be able to keep the scheduled appointment, the customer will be contacted as soon as possible and the appointment rescheduled to include updating the appointment in the Outlook Calendar.
4. If the Customer Support Technician reports for service at the scheduled time and the customer is not available:
   4.1. If no customer guidance or involvement is needed, the Customer Support Technician will:
       4.1.1. Complete the work per any existing Service Level Agreement and update the status of the work order in the Work Order System.
       4.1.2. Leave a note or message that the work has been completed.
   4.2. If customer guidance or involvement is needed, the Customer Support Technician will attempt to locate the customer or someone else in the office that can speak for the customer.
       4.2.1. If someone knowledgeable can be located, the Customer Support Technician will:
           4.2.1.1. Complete the work.
           4.2.1.2. Leave a note or message that the work has been completed.
       4.2.2. If someone knowledgeable cannot be located, the Customer Support Technician will:
           4.2.2.1. Leave a note or message that a Service Request was attempted, and request the Customer to call and reschedule.
4.2.2.2. Inform the Department of Information Technology Customer Support Team Lead and Assistant Director via email of the nature of the incident, name of the customer that could not be located and the customer’s Department. This email should be sent the same day as the incident.

5. If the Customer Support Technician reports for service at the scheduled time and the customer does not make the equipment available for service, requests rescheduling, or any other cause that prevents the Customer Support Technician from completing the Service Request, the Customer Support Technician will:

5.1. Inform the Customer to call and reschedule.

5.2. Inform the Department of Information Technology Customer Support Team Lead and Assistant Director via email of the nature of the incident, name of the customer involved and the customer’s Department. This email should be sent the same day as the incident.
Software Installation, Deployment, and Support on City Computers

11.1 Purpose
The purpose of this Policy and Procedure is to document the issues and responsibilities relevant to software installation, deployment, and support on all City of Montgomery computer systems.

11.2 Policy
It is the Policy of the City of Montgomery that all City-owned computers shall only contain legally licensed software that contributes to the productivity of employees in satisfying legitimate business needs of the City.

11.3 Applicability
This Policy and Procedure has been endorsed by the Mayor and is applicable to all City of Montgomery Departments.

11.4 Definitions
11.4.1 Authorized Software
Authorized Software is legally licensed software on City computers necessary for the accomplishment of City business, and includes Departmental-Unique Software, Productivity Software, Single Purpose Software, and Standard Software. Other types of software such as utilities or browser enhancements may be authorized provided the software is legally licensed and does not conflict with any other computer program or resources. The Department of Information Technology does not support all Authorized Software.

11.4.2 Departmental-Unique Software
Departmental-Unique Software is legally licensed software generally installed on a small subset of the computers purchased by the City, typically to meet the business needs of a small number of employees or office(s). The Department of Information Technology may install Departmental-Unique Software, or this software may be installed by the individual Department in coordination with the Department of Information Technology. Support for Departmental-Unique Software is generally supplied by the installing Department. Examples of Departmental-Unique Software include, but are not limited to:
* Crime Index
* Financial
* Payroll
* Records Management System
* Selected GIS applications

11.4.3 Legally Licensed Software
Legally Licensed Software is software that is acquired, installed, maintained, and used in accordance with the manufacturer’s software license.

11.4.4 Productivity Software
Productivity Software is approved enabling software technology that allows employees to perform their assigned tasks. Departmental-Unique Software and Standard Software are examples of Productivity Software.

11.4.5 Single Purpose Software
Single Purpose Software is software performing basically a dedicated and unique service or function, such as radio frequency control software, E911 software, or parking deck software, and is not considered Productivity Software or Departmental-Unique Software. Typically, Single Purpose Software is run on a computer system dedicated solely for this function and no other function. Support for Single Purpose Software is generally provided by the using Department, frequently under contract from the manufacturer.

11.4.6 Software License
A Software License is a legal contract outlining the terms and conditions of how an individual, group, or company may install and/or use a particular piece of software. Most software is licensed in some fashion, even if the software is free. The license typically includes the number of computers that may use the software (frequently limited to one computer unless additional fees are paid); the type and cost of manufacturer support; how long the software may be used without paying additional fees; etc. The City, Departments, and/or individual employees may be held liable for violation(s) of applicable software licenses. Possession of a valid or legal compact disk (CD) containing the software does not automatically
grant permission to use the software. Additionally, software downloaded without any charge from the 
Internet does not automatically mean that the software is either free, installable on any machine, or has 
unlimited usage. Downloaded software has a license that must be honored, including payment of any 
applicable fees.

11.4.7 Standard Software
Standard Software is legally licensed and supported software generally installed on most City computers. 
The Department of Information Technology usually installs Standard Software. Examples of standard 
software include, but are not limited to:
* Adobe Reader
* Java
* Microsoft Internet Explorer
* Microsoft Office (Word, Excel, Outlook)
* Microsoft Windows
* Windows Media Player

11.4.8 Supported Software
Supported Software is the inventory of legally licensed software for which the Department of Information 
Technology can provide technical assistance. In general, Supported Software is software used on the 
majority of City computers. Standard Software and some Departmental-Unique Software are examples of 
supported software. As newer versions of Supported Software are released, support for older versions 
will eventually be curtailed. Single Purpose Software is generally not Supported Software.

11.4.9 Unauthorized Software
Unauthorized Software is any software that is not installed by, or in coordination with, the Department of 
Information Technology; not legally licensed; does not contribute to official City business needs; poses a 
security risk; impacts network performance; uses excessive computing resources; not authorized Single 
Purpose Software; individually or personally purchased software, whether legally licensed or not; or is 
otherwise not approved by the Department of Information Technology. Examples of unauthorized 
software include, but are not limited to:
* Flight simulators
* Gambling (whether for fun or profit)
* Games
* Music downloads
* Napster
* Peer-to-peer file sharing
* Tax software
* VPN (Virtual Private Network) software not installed and configured by the Department of Information 
Technology

11.4.10 Unsupported Software
Unsupported Software is unauthorized software or any software that does not fit the definition of 
“Supported Software.” Unsupported software is not eligible to receive any technical support from the 
Department of Information Technology and, if determined to cause a conflict with other software, will be 
removed by the Department of Information Technology. Examples of unsupported software include, but 
are not limited to:
* AOL software
* E-mail clients other than Microsoft Outlook
* Firefox
* Google, MSN, Yahoo, or other toolbar extensions
* Instant messaging
* Netscape
* OpenOffice
* Yahoo Toolbar

11.5 Procedures
11.5.1 Department of Information Technology
1. The Director is responsible for:
1.1. Acting as the Mayor’s agent for this Policy/Procedure.
1.2. Creating and maintaining this Policy/Procedure.
1.3. Ensuring all City Department Heads are informed about their responsibilities regarding this policy.
1.4. Informing Department Heads of violations of this Policy/Procedure within his/her respective Department.
1.5. Removing any unauthorized or unsupported software at his/her discretion to minimize City liability or correct any potential or real system performance issue.
1.6. Interpreting the applicability of this Policy/Procedure amongst Department Heads. If a mutual agreement cannot be reached, the Director will involve the necessary Executive Assistant(s) to the Mayor for a resolution.
1.7. Directing Department of Information Technology staff members on issues related to this Policy/Procedure.
1.9. Evaluating Department Head requests for potential software procurements to ensure compatibility, supportability, cost effectiveness, and standardization, and approving or disapproving the software in writing.

2. The Staff is responsible for:
2.1. Identifying to the Department of Information Technology Director any unauthorized or unsupported software discovered.
2.2. Removing unauthorized or unsupported software that is causing any conflict with any supported City software without the need for prior approval.
2.3. Removing unauthorized or unsupported software as directed by the Department of Information Technology Director or other Department Head.
2.4. Installing supported software on Departmental computers, with priority being given to Standard Software over Departmental-Unique Software.

11.5.2 Department Heads
All City of Montgomery Department Heads are responsible for:
1. Ensuring all of his/her Department’s employees are aware of and follows this Policy/Procedure.
2. Ensuring only legally licensed productivity software is installed on any Departmental computer.
3. Reimbursing from his/her Departmental budget all costs incurred due to the installation or usage of unauthorized software, including licensing fees, fines, and increased Department of Information Technology troubleshooting or maintenance charges.
4. Removing unauthorized software found on any Department computer.
5. Submitting a request to the Department of Information Technology to assist in the evaluation and/or selection of all computer software (with the exception of Single Purpose Software) before the software is purchased, especially if Department of Information Technology assistance or support will be required or expected.
6. Providing appropriate personnel actions for employees installing software in violation of the license agreement.

11.5.3 Finance Department
The Finance Department is responsible for reviewing all purchase requests containing software for compliance with this Policy/Procedure.
1. For purchase requests submitted by the Department of Information Technology, processing the request using normal purchasing procedures.
2. For purchase requests from other Departments:
2.1. Ensuring the submitting Department Head has requested Department of Information Technology evaluation and/or selection following paragraph 11.5.2, Step 5, and returning to the Department Head any purchase request found to be not in compliance.
2.2. Ensuring the Department of Information Technology has approved the software for installation on a City computer following paragraph 11.5.1, Step 1.9, and returning to the Department Head any purchase request found to be not in compliance.
2.3. For purchase requests found to be in compliance, processing the request using normal purchasing procedures.

11.5.4 City Employees
All City of Montgomery employees are responsible for:
1. Following the guidelines.
2. Identifying to his/her Department Head any unauthorized software found on a computer.
3. Removing any software as directed by the Department Head.
Support Outside of Regular Business Hours
10.1 Purpose
The purpose of this Policy and Procedure is to document expectations for Department of Information Technology staff when providing support outside of regular business hours.
10.2 Policy
It is the Department of Information Technology Policy to provide access to an Primary On-Call Technician outside of regular business hours by means of telephone number (334) 241-2149.
10.3 Applicability
This Policy and Procedure is applicable to all Department of Information Technology employees.
10.5 Procedures
10.5.1 Customer Support Team Lead
The Customer Support Team Lead will establish and publish the rotating work schedules (paragraph 8.5.3.1).
10.5.2 Primary On-Call Technician and Back-up Team Lead
The Primary On-Call Technician and Back-up Team Lead will:
1. Carry their assigned mobile telephones with them at all times.
2. Ensure their mobile telephone is turned on and charged at all times.
3. Answer customer service calls during non-business hours:
   3.1. Document the service request.
   3.2. For Level 1 Support requests, resolve the request over the telephone.
   3.3. For Level 2 Support requests:
      3.3.1. That are Urgent Priority requests, work stoppages, Senior City Staff Member, etc, escalate the issue for resolution to the right Department of Information Technology staff member per the Team Function Lists
      3.3.2. That are not Urgent Priority requests, defer response until the next business day.
4. Record the service call in the Work Order System no later than the beginning of the next business day, to include assignment of any deferred items.
10.5.3 Primary On-Call Technician
The Primary On-Call Technician will:
1. At the start of his/her rotation duty:
   1.1. Forward office telephone extension 2149 to his/her mobile telephone number (see paragraph 10.5.5).
   1.2. Forward his/her mobile telephone to the Back-up Team Lead’s mobile telephone number (see paragraph 10.5.6).
2. At the end of his/her rotation duty:
   2.1. Coordinate with the next scheduled Primary On-Call Technician in the duty roster to forward extension 2149 to the correct mobile number. A staff member is not relieved of this duty until the next Primary On-Call Technician has assumed the responsibility.
   2.2. Turn off call forwarding on his/her mobile telephone (see paragraph 10.5.6.3).
10.5.4 Back-up Team Lead
The Back-up Team Lead will:
1. At the start of his/her rotation duty, ensure the Primary On-Call Technician has forwarded his/her mobile telephone to the Back-up Team Lead’s mobile telephone number.
2. At the end of his/her rotation duty, ensure the next Primary On-Call Technician in the duty roster has forwarded his/her mobile telephone to the next Back-up Team Lead’s mobile telephone number.
3. In the absence of the Primary On-Call Technician, perform the functions of the Primary On-Call Technician.
10.5.5 Office Telephone Call Forwarding Procedures
10.5.5.1 Turn On or Change Call Forwarding
1. Press the telephone line button for extension 2149.
2. Dial #919 followed by the mobile telephone number.
3. Hang up.
10.5.5.2 Turn Off Call Forwarding
1. Press the telephone line button for extension 2149.
2. Dial #91.
3. Hang up.

10.5.6 BlackBerry 7100i Call Forwarding Procedures
The following procedures are applicable to programming call forwarding on the Nextel BlackBerry 7100i telephone.
* For this section, click means to quickly press and release the trackwheel button.
* Adapted from the BlackBerry 7100i User Guide, Version 4.1

10.5.6.1 Adding a New Call Forwarding Number
1. Press the Green Phone Button.
2. Scroll to a number to be forwarded and click.
3. Click New Number.
4. Type a phone number.
5. Press the Enter key.
6. Click the trackwheel.
7. Click Close.

10.5.6.2 Turning On Call Forwarding
1. Press the Green Phone Button.
2. Click and scroll to Options, then click again.
3. Click Call Forwarding.
4. Scroll to If Busy and click.
5. Click Change Number.
6. Highlight the telephone number to receive this type of call.
7. Click the trackwheel.
8. Click Save.
9. Scroll to If No Answer and click.
10. Click Change Number.
11. Highlight the telephone number to receive this type of call.
12. Click the trackwheel.
13. Click Save.
14. Scroll to If Unreachable and click.
15. Click Change Number.
16. Highlight the telephone number to receive this type of call.
17. Click the trackwheel.
18. Click Save.
19. Click the trackwheel.
20. Click Save.

10.5.6.3 Turning Off Call Forwarding
Follow the procedures in paragraph 10.5.6.2, changing the telephone number to receive the call back to your preferred default.
Virtual Private Network (VPN)

7.1 Purpose
The purpose of this Policy and Procedure is to document the policy for Virtual Private Networks within the City of Montgomery and the implementation procedures within the Department of Information Technology.

7.2 Policy
It is the Policy of the Department of Information Technology to safeguard the security of all Information Technology assets belonging to the City of Montgomery, including those assets accessible using a Virtual Private Network.

7.3 Applicability
This Policy and Procedure is applicable to all City of Montgomery Departments.

7.5 Procedures

7.5.1 Basic Guidance
1. VPN should be considered a “last resort” and used only when a connection using dedicated City resources cannot be, or is impractical to, establish.
2. VPN access should be limited to City of Montgomery owned computers. Access to non-City computers will be evaluated on a case-by-case basis by the Department of Information Technology Director.
3. VPN access will be limited to computers with high-speed broadband capability due to the high overhead associated with VPN security protocols. Dial-up access is not generally appropriate for VPN access.

7.5.2 Security Requirements
1. The Sponsoring Department:
   1.1. Is responsible for ensuring all appropriate security requirements and protocols are enforced on each computer with VPN access.
   1.2. Is responsible for ensuring all individuals using a VPN follow security procedures.
   1.3. All additional costs associated with VPN security and compliance.
   1.4. Notifying the Department of Information Technology when VPN is no longer required on a computer.
2. Each computer with VPN access will:
   2.1. Be granted VPN access for the minimum time necessary to accomplish the job, but for a period of time not to exceed one year.
   2.2. Use only the VPN access client supplied by the Department of Information Technology.
   2.3. Contain virus-checking software that is current and automatically updated with new virus signatures.
   2.4. Not, at any time, be connected to the City’s VPN while also using a separate dial-up or network connection.
   2.5. Be physically safeguarded to ensure no unauthorized person can access the City’s resources.

7.5.3 Requesting Access

7.5.3.1 City-owned Computers
1. The Director of the Sponsoring Department submits a written request for VPN access to the Department of Information Technology Director. This request shall include:
   1.1. Identification of the specific data and/or system for which access is required.
   1.2. Identification of the computer requiring VPN access.
   1.3. Name of the person that will be using the VPN access.
   1.4. Expected duration of the VPN need (not to exceed one year).
   1.5. Certification that the computer:
      1.5.1. Is, and will remain, in compliance with “Policy/Procedure 06-010: Software Installation, Deployment, and Support on City Computers.”
      1.5.2. Currently meets the Security Requirements specified in paragraph 7.5.2 above, including a description of how the virus software on that computer will be kept current.
2. The Department of Information Technology Director will review each Sponsoring Department request and will:
   2.1. Upon approval, arrange for the computer to be configured as specified in paragraph 7.5.4 below.
   2.2. Upon disapproval, return the request to the Sponsoring Department with an explanation.

7.5.3.2 Non-City Computers
1. The Director of the Sponsoring Department submits a written request for VPN access to the Department of Information Technology Director. This request shall include:
   1.1. Certification that a City-owned computer cannot be used in lieu of a non-City computer.
   1.2. Identification of the specific data and/or system for which access is required.
   1.3. Identification of the computer requiring VPN access, including:
       1.3.1. Make and model of the computer.
       1.3.2. Operating System, including version number.
       1.3.3. Virus software, including version number.
       1.3.4. Firewall, including version number.
   1.4. Name of the entity owning the computer.
   1.5. Name of the person that will be using the VPN access following “Policy/Procedure 06-011: Acceptable Use of City Computing Resources.”
   1.6. Expected duration of the VPN requirement (not to exceed one year). For VPN access being provided to a contractor, this date cannot be beyond the expiration of the current contract.
   1.7. Certification that the computer:
       1.7.1. Is, and will remain, in compliance with “Policy/Procedure 06-010: Software Installation, Deployment, and Support on City Computers.”
       1.7.2. Currently meets the Security Requirements specified in paragraph 7.5.2 above, including a description of how the virus software on that computer will be kept current.
2. The Department of Information Technology Director will review each Sponsoring Department request and will:
   2.1. Upon approval, arrange for the computer to be configured as specified in paragraph 7.5.4 below.
   2.2. Upon disapproval, return the request to the Sponsoring Department with an explanation.
7.5.4 VPN Configuration
The Department of Information Technology will:
1. Verify the computer is compatible with the software necessary to establish secure VPN access.
2. Verify the computer meets required security standards as specified in paragraph 7.5.2.
3. Install the software necessary to establish secure VPN access.
4. Provide the person that will be using the VPN:
   4.1. The necessary user identification and password.
   4.2. Training on using the VPN.
7.5.5 Continued Access
If the requirement for VPN access continues beyond the expected duration specified in the initial VPN request, the Director of the Sponsoring Department submits a new request following the procedures in paragraph 7.5.3 above.
CONFIDENTIALITY STATEMENT
I, ________________, acknowledge and understand that in the course of my employment, I may be provided access to highly confidential information in order to perform my job. I must keep in mind at all times that the City’s confidential information is unique and of significant value and must always remain the property of the City.

All confidential information of the City, including, but not limited to, disciplinary files, financial data, personnel and health related files, and police department records, is and will remain confidential. Disclosure to anyone outside the City [unless authorized in writing by a Department Director] is strictly and absolutely prohibited.

I agree to keep any and all information to which I have access during the course of my employment with the City in strictest confidence and to never discuss or disclose any said information to any other person who does not otherwise clearly have access to the information during the course of their employment with the City.

I understand that during and after my employment with the City that I am forbidden to remove or cause to be removed from City premises, for purposes other than for work or assignments for the City, any materials belonging to the City, including documents, materials or files created, discovered, produced or developed for or by the City unless I am authorized in writing to do so by a Department Director. Upon termination of my employment for whatever reason, I understand and acknowledge that I must immediately surrender to the City all documents, notebooks, records, files, disks and copies of such items as well as any and all other property which belongs to the City. I understand, acknowledge and agree that I am prohibited from making or retaining any copies of any such materials or any City property following my separation from employment.

I further acknowledge that violation of this policy will cause irreparable injury to the City and that violation during the course of my employment will subject me to discipline, up to and including termination.
In an effort to provide a comfortable but business-like environment for ‘Dress Down Friday’ the following guidelines are put forth as acceptable.

**Head Accessories**

* No hats or caps indoors.
* No sunglasses may be worn indoors, except for medical reasons.
* All head attire for medical or religious reasons is permitted.

**Shirts, Tops, Blouses, and Jackets**

* Casual shirts, collared polo shirts, button-down shirts, blouses, sweaters and St. Lucie County t-shirts are acceptable.
* Inappropriate attire includes tank tops; midriff baring tops; shirts with other county’s logos; shirts with potentially offensive words, terms, logos, pictures, cartoons, or slogans; halter-tops; low-cut tops and tops with bare shoulders.

**Slacks, Jeans, Pants**

* Slacks, jeans, gauchos and capris are acceptable in the office. Pants that are below the knee with finished edges are allowed. All acceptable pants must be clean and without tears.
* Inappropriate slacks or pants in the office include, sweatpants, exercise pants, short shorts, low-cut jeans, shorts, Bermuda shorts, leggings, and any spandex or other type of form-fitting pants such as clothing worn for biking. As a general rule, shorts or pants that are above knee length are not allowed.

**Skirts, Dresses, and Skirted Suits**

* Casual dresses and skirts, and skirts that are split at or below mid thigh are acceptable. As a general rule, dresses and skirts should be below mid-thigh length.
* As a general rule, dresses and skirts that are above mid-thigh length are not allowed. Short, tight skirts that are above mid-thigh are inappropriate for work. Mini-skirts, shorts, sun dresses, beach dresses, bathing suit cover-ups, and spaghetti-strap dresses are inappropriate for the office.

**Shoes and Footwear**

* Loafers, boots, dress shoes, dress sandals, and leather deck shoes, as examples, are acceptable. All footwear must be free of stains, tears, paint, etc.
* Work boots, dirty athletic shoes, thongs, flip-flops, slippers are unacceptable.
Wireless Network Usage and Access Policy

Purpose: The purpose of this policy is to provide guidelines for access to Columbia County Board of Commissioners’ network via wireless connectivity.

Scope: This policy applies to all County employees, consultants, and 3rd party vendors who may access Columbia County’s wireless network.

Policy:
1. Only approved wireless adaptors will be permitted to access Columbia County’s wireless network.
2. Adaptors will be issued by Columbia County’s IT department only at the request of the department head or division director by submitting a signed work order request with IT Helpdesk.
3. Departments will be responsible for all costs incurred by the purchased of wireless adaptors for permanent assignment to that department.
4. Adaptors may be borrowed from Columbia County IT department for an 8 business hour period. Eight business hour notice must be provided to the IT Helpdesk by submitting a signed work order request to IT Helpdesk. Only a limited number of wireless adaptors will be available. If cards are not returned in approved amount of time, the department manager will be notified.
5. Wireless adaptor software will be configured by Columbia County IT staff with appropriate security settings.
6. Vendors may use Columbia County’s wireless network to access the Internet only. Vendors will be provided the security required to access the Internet through the County wireless network. Eight business hour notice must be given to the IT Helpdesk for vendor configuration.
7. Vendor security settings will be changed on a regular basis.
8. Employee security settings may be changed as needed. All users with permanent wireless adaptors will be contacted by Columbia County IT in order schedule a time to make necessary changes on the wireless adaptor software.
9. All computers connected to Columbia County’s network via wireless must comply with the Columbia County wireless policy and all applicable Columbia County Security policies
10. If a wireless adaptor becomes lost or stolen, it will be the responsibility of the borrower to replace the item.
11. Users must sign and agree to the wireless policy before use.
12. Employees and vendors will be limited to the resources to which they need access.
13. It is the responsibility of users with wireless privileges to ensure that unauthorized persons are not allowed access to Columbia County’s internal network.
14. Only Columbia County IT staff has the authority to install wireless access points. Any unauthorized access points will be immediately disconnected and Columbia County IT staff will take possession of the unit. All information of unauthorized access point will be routed to the proper authorities to investigate.
15. This policy is subject to change.

Enforcement: Any user found in violation of this policy will subject to, but not limited to, loss of wireless connectivity privileges.

I have read the Columbia County’s Wireless Network Usage and Access Policy. I fully understand this policy and agree to abide by its terms. I understand that the release of Columbia County confidential information, the loss of data or loss of equipment through my failure to comply with these requirements, or any unauthorized use of my access may subject me to disciplinary action up to and including termination.
102 St. Lucie County, FL – Work Order Request Procedure

Work Order Request Procedure
1.0 PURPOSE
The purpose of this document is to provide a methodology whereby customers can get their requests logged and tracked so SLC IT can manage resources, follow standard industry practices and provide feedback to the customer.

2.0 POLICY
All requests for any type of SLC IT service from BOCC or supported agencies must go through Customer Service to be put into a work order for internal record keeping and to provide a means of reference in order to provide feedback. Requests can be made via phone, email, Intranet or face-to-face.

3.0 PROCEDURE
Call Customer Service at x2146, email at Customer@stlucieco.gov or use the Intranet at http:
Cleaning the LCD Display
MAKE SURE THE LCD DISPLAY IS TURNED OFF. NEVER SPRAY OR POUR ANY LIQUID DIRECTLY ONTO THE SCREEN OR CASE.
To clean the screen:
1. Wipe the screen with a clean, soft, lint-free cloth. This removes dust and other particles.
2. If the screen is still not clean, apply a small amount of non-ammonia, non-alcohol based glass cleaner onto a clean, soft, lint-free cloth, and wipe the screen.
3. As an alternative, apply a small amount of warm soap water onto a clean, soft, lint-free cloth, and wipe the screen.
To clean the case:
1. Use a soft, dry cloth.
2. If the case still not clean, apply a small amount of a non-ammonia, non-alcohol based, mild non-abrasive detergent onto a clean, soft, lint-free cloth, then wipe the surface.
Disclaimer: Information Technology does not recommend the use of any ammonia or alcohol-based cleaners on the LCD display screen or case. Some chemical cleaners have been reported to damage the screen and/or case of the LCD display. Information Technology will not be liable for damage resulting from use of any ammonia or alcohol-based cleaners.
Questions: If you have any questions or would like further guidance, please call Information Technology Customer Service at 462-2146.
PROCEDURE AND POLICY FOR HIRING EMPLOYEES

* Applicant MUST complete a standard St. Lucie County Board of County Commissioners Employment application. No exceptions.
* All applications MUST come to, be logged in and approved by Human Resources BEFORE departments can consider the applicant for employment. No exceptions.
* If a department is interested in an applicant, an interview should be given.
* Consideration should be given to qualified applicants who are claiming Veteran's Preference (FS 295.07)
* If the department wishes to hire the person, at least two reference checks/verifications of employment must be completed. Forms for telephone reference checks can be found on the intranet under Human Resources. This is done at the department level so that you have the opportunity to get as much information as you can about your potential employee, (whether positive or negative) This way you can make an informed decision based on information that you’ve received from outside sources.
* If not interested in an applicant that you’ve interviewed, a letter should be sent to the person notifying them of your decision. Sample letter is available on the Intranet under Human Resources.
* If still interested in proceeding, attach the completed references to a memo stating your intention to hire the person and send to Human Resources as soon as possible. Human Resources will then perform a Criminal Background Check as well as a check of the applicant’s current Driving Record. The application and background information will be reviewed by the Director of Human Resources as well as the Assistant County Administrator.
* If approval has not been granted, a letter should be sent to thank the person for applying. Sample letter is available on the Intranet under Human Resources.
* Once their approval has been granted, the department can offer the applicant a position contingent upon a pre-employment physical and drug screen. A phone call followed by a letter is recommended. Under no circumstance should anyone encourage a person to give a notice to their current employer at this point.
* Notify Human Resources of acceptance of offer. We will then schedule the necessary appointment at the Health Department with the applicant.
* Once the Health Department gives their approval, Human Resources will notify the department and the applicant. A start date and orientation will be scheduled. Start dates are always on a Monday and orientations are held on the first Monday and Tuesday of their employment. Information for payroll purposes will be forwarded to the appropriate personnel.
Virtual Private Network Usage and Access Policy

Purpose: The purpose of this policy is to provide guidelines for Remote Access IPSec Virtual Private Network (VPN) connections to the Columbia County Board of Commissioners network.

Scope: This policy applies to all County employees, consultants, and 3rd party vendors who may access Columbia County's network via VPN.

Policy
1. VPN provides secure access into Columbia County Government's network. VPN does not provide Internet connectivity. Users are responsible for providing their own Internet service via dial-up, cable modem, DSL, or other means in order to use Columbia County’s VPN service.
2. VPN clients will only be installed on Columbia County issued pcs or laptops. The VPN client will not be supported on individual user’s home pcs.
3. User accounts will be created only at the request of the department head or division director by submitting a signed work order request to the IT Helpdesk.
4. Accounts for non-Columbia County employees must be approved by the Management Services Director. Non-Columbia County employees must comply with all Columbia County security policies.
5. Users must sign and agree to the VPN policy before use.
6. Employees and vendors will be limited to the resources to which they need access.
7. It is the responsibility of users with VPN privileges to ensure that unauthorized persons are not allowed access to Columbia County’s internal network.
8. VPN Access will be controlled by a secure username and password. Shared accounts are not permitted.
9. Only Columbia County IT approved VPN clients and operating systems are permitted. Refer to the IT standards document for updated list.
10. Users will be disconnected after 30 minutes of inactivity.
11. All users are subject to auditing.
12. This policy is subject to change.

Enforcement: Any user found in violation of this policy will subject to, but not limited to, loss of VPN privileges.

I have read the Columbia County’s Virtual Private Network Usage and Access Policy. I fully understand this policy and agree to abide by its terms. I understand that the release of Columbia County confidential information, the loss of data or loss of equipment through my failure to comply with these requirements, or any unauthorized use of my access may subject me to disciplinary action up to and including termination.
Please complete this form as soon as possible and return to Human Resources. We have been informed
that the last day of employment for the referenced employee is:
The employee must return all assigned department equipment, uniforms, etc. and all County identification
cards and health insurance cards (if applicable) before receiving their final paycheck.

DEPARTMENT ADMINISTRATOR/DIVISION DIRECTOR:
Please place a check beside the items returned:
badges ____, uniforms ____, department equipment ____, keys ____,
priority one cards _____, cell phone ________, beeper ________
County credit card ________, fuel authorization ________, gate authorization ________.
employee handbook _____, health handbook ________.
List any items due and costs, etc.:
IMMEDIATE SUPERVISOR'S COMMENTS:
Reason of termination: Retirement _____ Resignation _____ Discharge _____ Layoff _____
Would you consider for rehire?
Name of immediate supervisor:
HUMAN RESOURCES USE
1. Exit Interview Form completed?
2. County ID Card returned?
3. Health Insurance ID Card(s) returned?
4. Date County Health Insurance expires:
copies: Payroll _______ Insurance _______ Department _______ Information Technology (Customer
Service) Employee File ________ Service Garage _______ Purchasing ________
KWIC INDEX TO GMIS POLICIES
other types of leave including leave of ABSENCES, time sheets or timecards along with 0008:0106
operate to waive, destroy, impair, or ABSOLVE the rights or obligations of the City 0009:0136
Access ABUSE 0003:0105
modification, destruction or ABUSE The Division of Information & 0053:019
vaccinations certificates, neglect or ABUSE cases which have not resulted in 0008:0461
e.g., inappropriate conduct, ABUSE of privileges or rights, workplace 0032:0049
or proprietary information, personal ABUSE of the system or monitoring workflow 0002:0020
to answer their department's call and ABUSE the voice mail system, could result in 0029:0010
Data Processing for impropriety and/or ABUSES 0003:0146
work. Any employee that is reported ABUSING the browsing privileges will be subject 0002:0087
be harassing, libelous, threatening, ABUSIVE foul, or obscene 0060:0031
upload or download any disruptive, ABUSIVE harassing, threatening, or offensive 0003:0123
infringe upon the rights of others. No ABUSIVE profane or offensive language is 0061:0009
send or receive threatening, obscene, ABUSIVE sexually explicit language or 0055:0043
offensive, ABUSIVE threatening, or other inappropriate 0071:0014
amount of time spent on those sites. following guidelines are put forth as ACCEPTABLE 0100:0001
11. Limited personal use is ACCEPTABLE as long as the overseeing Row Officer 0090:0102
regard. The following are examples of ACCEPTABLE exceptions to this policy 0095:0014
the County's network to the Internet ACCEPTABLE in small limited amounts as long as it 0002:0087
must, even on Casual Day, portray an ACCEPTABLE level of business professionalism 0002:0087
important resource by outlining its ACCEPTABLE use always is lawful, ethical, reflects 0003:0081
policies takes precedence over ACCEPTABLE use, as well as defining certain 0005:0003
Information Technology Policy - ACCEPTABLE use policies of those other systems 0068:0008
Procedures and Standards - ACCEPTABLE Use 0062:0001
file copy of the employee's signed ACCEPTABLE Use 0065:0001
Policies and Procedures for the ACCEPTABLE Use Agreement 0052:0001
following "Policy/Procedure 06-011: ACCEPTABLE Use Agreement 0054:0013
PDA that would violate the Village's ACCEPTABLE Use of Computers and Technology 0069:0001
E-mail ACCEPTABLE Use of City Computing Resources 0091:0001
System can be found in the E-Mail ACCEPTABLE Use of City Computing Resources 0098:0055
(as defined by the Village's Internet ACCEPTABLE Use Policy the Village will seek to 0031:0015
Request procedure; section IV.B of the ACCEPTABLE Use Procedures 0066:0009
A. ACCEPTABLE Use Standards: Acceptable uses for 0007:0014
1. ACCEPTABLE Use of the Internet ACCEPTABLE Use of the Internet 0007:0004
Policy and Procedure supersedes the " ACCEPTABLE USE Policy for Computer Network and 0091:0004
so a log can be made of the ACCEPTABLE Policy and Procedure supersedes the 0069:0211
a. ACCEPTED acts, e.g., input errors and omissions 0032:0047
related to their specific use, i.e. ACCEPTED beverage spills, improper ventilation 0002:0243
site on the internet is accessed ACCEPTED the user should 0069:0208
or controls that could be ACCEPTED triggered or intentionally exploited 0032:0055
ACCIDENTAL computer equipment malfunction 0022:0024
and penalties; loss of licensure or ACCEPTED professional, GeneXus .NET 0002:0300
regulations, professional ethics, and ACCEPTED Professional, GeneXus .NET 0002:0300
regulations, professional ethics, and ACCREDITATION requirements 0047:0018
products, Dreamweaver, Formium, Adobe ACCREDITATION requirements 0048:0015
agreement with a vendor (e.g., SCT, ACCROBAT Professional, GeneXus .NET 0002:0300
sent from a Gaston County email ACS Printtrak); provided however, that any 0015:0005
required to disclose his or her name ADDRESS or phone number. However, if a written 0002:0055
personal information (telephone, ADDRESS , social security numbers) for law 0004:0036
Head's approval to request an E-mail ADDRESS . By doing this, you will limit the 0053:0013
who know your County e-mail ADDRESS Passwords must not be a word found in 0090:0161
plate number, a spouse's name, or an ADDRESS "Work ADDRESS 0085:0024
"Technology Usage Procedures." to ADDRESS and communicate existing and new 0003:0003
everyone who has a County E-Mail ADDRESS and is maintained by Information 0010:0004
to IT system and will assign an email ADDRESS and/or voice mailbox to me based upon 0089:0020
11. The maintenance of the master ADDRESS and public group lists used on the 0016:0016
ADDRESS and telephone number changes 0091:0013
** Routine ADDRESS is: "Pagers - On Call for IT Techs" 0019:0004
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>security measures and safeguards to</td>
<td>ADDRESS</td>
<td>key vulnerabilities. To accomplish</td>
<td>0032:0085</td>
</tr>
<tr>
<td>when IT vendors release fixes to</td>
<td>ADDRESS</td>
<td>known bugs or problems...</td>
<td>0044:0016</td>
</tr>
<tr>
<td>content. In addition, having an e-mail</td>
<td>ADDRESS</td>
<td>on the Internet may lead to receipt of</td>
<td>0069:0207</td>
</tr>
<tr>
<td>basis. Periodic reminders shall</td>
<td>ADDRESS</td>
<td>password security, malicious software,...</td>
<td>0035:0022</td>
</tr>
<tr>
<td>development team member should</td>
<td>ADDRESS</td>
<td>the call in the following manner:</td>
<td>0014:0024</td>
</tr>
<tr>
<td>at the facility. Such procedures shall</td>
<td>ADDRESS</td>
<td>the following:</td>
<td>0039:0023</td>
</tr>
<tr>
<td>This Policy/Procedure attempts to</td>
<td>ADDRESS</td>
<td>the roles and responsibilities of</td>
<td>0093:0017</td>
</tr>
<tr>
<td>additional steps shall be taken to</td>
<td>ADDRESS</td>
<td>the security of the associated</td>
<td>0034:0036</td>
</tr>
<tr>
<td>by employees from a Martin County email</td>
<td>ADDRESS</td>
<td>to newsgroups must contain a disclaimer.</td>
<td>0005:0017</td>
</tr>
<tr>
<td>Browser products, Dreamweaver, Formum,</td>
<td>ADOBE</td>
<td>Acrobat Professional, GeneXus.NET</td>
<td>0020:0030</td>
</tr>
<tr>
<td>*</td>
<td>ADOBE</td>
<td>Reader</td>
<td>0092:0194</td>
</tr>
<tr>
<td>*</td>
<td>ADOBE</td>
<td>Reader</td>
<td>0096:0037</td>
</tr>
<tr>
<td>ADVERTISEMENTS: LEGAL (Required ads and/or announcements from newspapers)</td>
<td>ADS</td>
<td>sexually explicit, violence, criminal</td>
<td>0065:0013</td>
</tr>
<tr>
<td>fall into the following categories:</td>
<td>ADULT</td>
<td>/sexually explicit, violence, criminal</td>
<td>0065:0013</td>
</tr>
<tr>
<td>service providers on behalf of, or to</td>
<td>ADVERTISE</td>
<td>and promote departmental programs.</td>
<td>0008:0094</td>
</tr>
<tr>
<td>public functions that are designed to</td>
<td>ADVERTISE</td>
<td>items for sale is not acceptable.</td>
<td>0090:0103</td>
</tr>
<tr>
<td>to participate in chain letters or to</td>
<td>ADVERTISEMENTS</td>
<td>is frequently filed with the item to</td>
<td>0008:0010</td>
</tr>
<tr>
<td>the transmission or storage of private</td>
<td>ADVERTISEMENTS</td>
<td>personal opinions or personal</td>
<td>0016:0013</td>
</tr>
<tr>
<td>part of another record series. A legal</td>
<td>ADVERTISEMENTS</td>
<td>opinions or personal</td>
<td>0026:0024</td>
</tr>
<tr>
<td>to, those messages containing personal</td>
<td>ADVERTISEMENTS</td>
<td>solicitations, promotions, destructive</td>
<td>0008:0094</td>
</tr>
<tr>
<td>to, those messages containing personal</td>
<td>ADVERTISEMENTS</td>
<td>personal opinions or personal</td>
<td>0016:0013</td>
</tr>
<tr>
<td>or storing commercial or personal</td>
<td>ADVERTISEMENTS</td>
<td>opinions or personal</td>
<td>0026:0024</td>
</tr>
<tr>
<td>limited to, distribution of unsolicited</td>
<td>ADVERTISING</td>
<td>propagation of computer &quot;worms&quot; and...</td>
<td>0003:0129</td>
</tr>
<tr>
<td>the sending of &quot;junk mail&quot; or other</td>
<td>AERONAUTICS</td>
<td>material to individuals who did not</td>
<td>0005:0039</td>
</tr>
<tr>
<td>of Public Works, and Department of</td>
<td>TAPES</td>
<td>may establish user connectivity to</td>
<td>0065:0047</td>
</tr>
<tr>
<td>up Monday through Friday on 50/100 GB</td>
<td>ALERT</td>
<td>Tapes. Backups are done using Arcserve</td>
<td>0075:0008</td>
</tr>
<tr>
<td>(mobile phone), or by Direct Connect</td>
<td>ALERT</td>
<td>3813. Please allow 30 minutes for a...</td>
<td>0019:0005</td>
</tr>
<tr>
<td>Higher ALERT</td>
<td>Status</td>
<td>0049:0087</td>
<td></td>
</tr>
<tr>
<td>Courthouse Security should be</td>
<td>ALERTED</td>
<td>to the threat; such threat can be</td>
<td>0032:0071</td>
</tr>
<tr>
<td>care providers previously have been</td>
<td>ALERTED</td>
<td>than normal. This will be done in...</td>
<td>0049:0089</td>
</tr>
<tr>
<td>requested to go to a higher status of</td>
<td>ALERTING</td>
<td>set, logging functions turned on, and...</td>
<td>0040:0031</td>
</tr>
<tr>
<td>features will be enabled, full</td>
<td>ALPHA</td>
<td>character and at least one being</td>
<td>0002:0188</td>
</tr>
<tr>
<td>characters long, the first being an</td>
<td>ALPHABETIC</td>
<td>characters,</td>
<td>0035:0053</td>
</tr>
<tr>
<td>1) Upper case</td>
<td>ALPHABETICAL</td>
<td>which is located away from the...</td>
<td>0008:0076</td>
</tr>
<tr>
<td>of a subject file, generally filed</td>
<td>ALPHANUMERIC</td>
<td>and special characters</td>
<td>0006:0031</td>
</tr>
<tr>
<td>in length, using a combination of</td>
<td>ALPHANUMERIC</td>
<td>characters long, the first being an...</td>
<td>0002:0188</td>
</tr>
<tr>
<td>* Are at least eight</td>
<td></td>
<td>characters</td>
<td>0090:0158</td>
</tr>
<tr>
<td>must be comprised of a minimum of 8</td>
<td>ANTI</td>
<td>Virus Protection</td>
<td>0003:0210</td>
</tr>
<tr>
<td>7.2 network must pass through the Norton</td>
<td>ANTI-VIRUS</td>
<td>for Exchange before it is allowed to...</td>
<td>0076:0021</td>
</tr>
<tr>
<td>any authorized encryption device, or</td>
<td>ANTI-VIRUS</td>
<td>or other software program, installed on...</td>
<td>0055:0027</td>
</tr>
<tr>
<td>relies exclusively on the Workstation</td>
<td>ANTI-VIRUS</td>
<td>scan. This by-pass control...</td>
<td>0007:0012</td>
</tr>
<tr>
<td>available) and updating by a central</td>
<td>ANTI-VIRUS</td>
<td>server.</td>
<td>0068:0229</td>
</tr>
<tr>
<td>Requirement 5: Use and regularly update</td>
<td>ANTI-VIRUS</td>
<td>software and how to check a workstation...</td>
<td>0035:0032</td>
</tr>
<tr>
<td>b. The importance of updating</td>
<td>ANTI-VIRUS</td>
<td>Software: Ensure anti-virus software on...</td>
<td>0065:0054</td>
</tr>
<tr>
<td>C.4. These worms may not be detectable by</td>
<td>ANTI-VIRUS</td>
<td>software. As a result, the use of free...</td>
<td>0002:0733</td>
</tr>
<tr>
<td>7. Install Corporate Edition Norton</td>
<td>ANTIVIRUS</td>
<td>protection on the laptops. County...</td>
<td>0003:0226</td>
</tr>
<tr>
<td>and maintains a license for an</td>
<td>ANTIVIRUS</td>
<td>software (set to run automatically)...</td>
<td>0085:0015</td>
</tr>
<tr>
<td>Always make sure that you have current</td>
<td>ANTIVIRUS</td>
<td>software-All vulnerable servers run...</td>
<td>0076:0022</td>
</tr>
<tr>
<td>Running server and workstation</td>
<td>ANTIVIRUS</td>
<td>software on all workstations to detect...</td>
<td>0044:0017</td>
</tr>
<tr>
<td>will install and regularly update</td>
<td>ANTIVIRUS</td>
<td>software or could arrive prior to an...</td>
<td>0035:0036</td>
</tr>
<tr>
<td>a potential virus that could sneak past</td>
<td>ANTIVIRUS</td>
<td>Suites...</td>
<td>0002:0301</td>
</tr>
<tr>
<td>unauthorized messaging software such as</td>
<td>AOL</td>
<td>YAHOO, Windows Messenger; and...</td>
<td>0003:0118</td>
</tr>
<tr>
<td>use through various sites such as MSN,</td>
<td>AOL</td>
<td>and YAHOO. With this growth has come...</td>
<td>0002:0733</td>
</tr>
<tr>
<td>*</td>
<td>AOL</td>
<td>software</td>
<td>0092:0238</td>
</tr>
<tr>
<td>*</td>
<td>AOL</td>
<td>software</td>
<td>0096:0060</td>
</tr>
</tbody>
</table>
### KWIC INDEX TO GMIS POLICIES

<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>and dating, glamour and intimate APPAREL</td>
<td>Glamour &amp; Intimate APPAREL</td>
<td>drugs and alcohol, hacking, remote</td>
<td>0082:0021</td>
</tr>
<tr>
<td>case letters, a, b, (iii) Westernized ARABIC</td>
<td>case letters, a, b, (iii) Westernized ARABIC</td>
<td>numerals, 0,1,2, and (iv)</td>
<td>0003:0025</td>
</tr>
<tr>
<td>contracts, leases or agreements with ARCHITECTS</td>
<td>* Description of the software, except for backup and ARCHIVAL</td>
<td>engineers, builders, and construction</td>
<td>0008:0356</td>
</tr>
<tr>
<td>creation to ultimate destruction or ARCHIVAL</td>
<td>and technologies that are used by the ARCHIVAL</td>
<td>Backup and Storage Policy</td>
<td>0002:0538</td>
</tr>
<tr>
<td>is encouraged. These records may have ARCHIVAL</td>
<td>value. ARCHIVAL</td>
<td>any emails and to save any attachments.</td>
<td>0008:0094</td>
</tr>
<tr>
<td>30 days, and then deleted. PC Users may ARCHIVE</td>
<td>30 days, and then deleted. PC Users may</td>
<td>阿根廷</td>
<td>0002:0581</td>
</tr>
<tr>
<td>After that period, tape media used to ARCHIVE</td>
<td>After that period, tape media used to</td>
<td>stored, distributed, edited or</td>
<td>0003:0169</td>
</tr>
<tr>
<td>sexually explicit material may not be ARCHIVED</td>
<td>sexually explicit material may not be</td>
<td>elsewhere</td>
<td>0009:1919</td>
</tr>
<tr>
<td>and dating, glamour and intimate APPAREL</td>
<td>and dating, glamour and intimate APPAREL</td>
<td>hacking, remote</td>
<td>0002:0581</td>
</tr>
<tr>
<td>County may access user files, including ARCHEV</td>
<td>County may access user files, including</td>
<td>material of present and former</td>
<td>0002:0050</td>
</tr>
<tr>
<td>Florida Department of State: Bureau of ARCHIVES</td>
<td>Florida Department of State: Bureau of</td>
<td>Archives and Records Management</td>
<td>0004:0056</td>
</tr>
<tr>
<td>Public Records Administrator and State ARCHIVES</td>
<td>Public Records Administrator and State</td>
<td>as it may be amended from time to time</td>
<td>0008:0300</td>
</tr>
<tr>
<td>Gaston County computers, for other than ARCHIVING</td>
<td>Gaston County computers, for other than</td>
<td>purposes, is prohibited</td>
<td>0002:0356</td>
</tr>
<tr>
<td>Date of Record</td>
<td>ARCHIVING</td>
<td>tasks associated with paper-based</td>
<td>0002:0055</td>
</tr>
<tr>
<td>Adobe, rich text files, HTML, XML, ASP.</td>
<td>Adobe, rich text files, HTML, XML, ASP.</td>
<td>tasks associated with paper-based</td>
<td>0002:0055</td>
</tr>
<tr>
<td>This information, like any other ASSET</td>
<td>This information, like any other</td>
<td>must be protected</td>
<td>0009:0005</td>
</tr>
<tr>
<td>be treated as though it is a County ASSET</td>
<td>be treated as though it is a County</td>
<td>and a critical component</td>
<td>0002:0102</td>
</tr>
<tr>
<td>Voice mail is a Gaston County ASSET ASSET</td>
<td>Voice mail is a Gaston County</td>
<td>in the software register. However,</td>
<td>0008:0004</td>
</tr>
<tr>
<td>and record it as an organization-owned ASSET</td>
<td>and record it as an organization-owned</td>
<td>inventory data collection, data</td>
<td>0003:0047</td>
</tr>
<tr>
<td>PCs has occurred, use the County's Fixed ASSET</td>
<td>PCs has occurred, use the County's Fixed</td>
<td>Management Specialist in Administrative</td>
<td>0006:0020</td>
</tr>
<tr>
<td>Managing Information and Technology ASSETS</td>
<td>Managing Information and Technology</td>
<td>number (FA#) to try to find who has the</td>
<td>0005:0028</td>
</tr>
<tr>
<td>* Maximize County ASSETS</td>
<td>* Maximize County</td>
<td>must be protected from release to</td>
<td>0006:0004</td>
</tr>
<tr>
<td>County records are information ASSETS</td>
<td>County records are information</td>
<td>and must be accessible to the full</td>
<td>0057:0003</td>
</tr>
<tr>
<td>workplace violence, waste of corporate ASSETS</td>
<td>workplace violence, waste of corporate</td>
<td>harassment</td>
<td>0032:0049</td>
</tr>
<tr>
<td>of Bradford County's Information ASSETS</td>
<td>of Bradford County's Information</td>
<td>Each system may, at times, have its</td>
<td>0008:0001</td>
</tr>
<tr>
<td>are implemented to protect the Town's ASSETS</td>
<td>are implemented to protect the Town's</td>
<td>if you feel that the level of</td>
<td>0060:0019</td>
</tr>
<tr>
<td>County invests in and uses computer ASSETS</td>
<td>County invests in and uses computer</td>
<td>(computer hardware, software,</td>
<td>0002:0007</td>
</tr>
<tr>
<td>computers are organization-owned ASSETS</td>
<td>computers are organization-owned</td>
<td>must be kept both software legal</td>
<td>0058:0052</td>
</tr>
<tr>
<td>of Charleston County's key information ASSETS</td>
<td>of Charleston County's key information</td>
<td>Charleston County is</td>
<td>0003:0409</td>
</tr>
<tr>
<td>security of all Information Technology ASSETS</td>
<td>security of all Information Technology</td>
<td>belonging to the City of Montgomery</td>
<td>0098:0007</td>
</tr>
<tr>
<td>a. Identify all ASSETS</td>
<td>a. Identify all</td>
<td>potentially compromised by the</td>
<td>0036:0029</td>
</tr>
<tr>
<td>&amp; availability of the information</td>
<td>&amp; availability of the information</td>
<td>you have access to</td>
<td>0059:0011</td>
</tr>
<tr>
<td>for the content of all text, audio</td>
<td>for the content of all text, audio</td>
<td>, or images that they place or send or</td>
<td>0061:0009</td>
</tr>
<tr>
<td>or retrieve any materials (video or</td>
<td>or retrieve any materials (video or</td>
<td>that could be considered inappropriate</td>
<td>0040:0023</td>
</tr>
<tr>
<td>are not allowed to play streaming</td>
<td>are not allowed to play streaming</td>
<td>on the County's Network</td>
<td>0002:0087</td>
</tr>
<tr>
<td>the use of such services as streaming</td>
<td>the use of such services as streaming</td>
<td>on the County's Network</td>
<td>0002:0087</td>
</tr>
<tr>
<td>(to include downloaded screen savers), audiovisual auditory</td>
<td>(to include downloaded screen savers), audiovisual auditory</td>
<td>on the County's Network</td>
<td>0002:0087</td>
</tr>
<tr>
<td>OFFICIAL MEETINGS (HANDWRITTEN/</td>
<td>OFFICIAL MEETINGS (HANDWRITTEN/</td>
<td>audiovisual auditory</td>
<td>0008:0256</td>
</tr>
<tr>
<td>software, compact discs, videotapes,</td>
<td>software, compact discs, videotapes,</td>
<td>audiovisual auditory</td>
<td>0008:0256</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>audiovisual auditory</td>
<td>0023:0010</td>
</tr>
<tr>
<td>still images, and motion pictures and</td>
<td>still images, and motion pictures and</td>
<td>audiovisual auditory</td>
<td>0025:0010</td>
</tr>
<tr>
<td>to exercise the right to review,</td>
<td>to exercise the right to review,</td>
<td>audiovisual auditory</td>
<td>0058:0021</td>
</tr>
<tr>
<td>and will exercise the right to review,</td>
<td>and will exercise the right to review,</td>
<td>intercept, access and disclose</td>
<td>0060:0055</td>
</tr>
<tr>
<td>County reserves the right to review,</td>
<td>County reserves the right to review,</td>
<td>County reserves the right to review,</td>
<td>0052:0024</td>
</tr>
<tr>
<td>the right to review,</td>
<td>the right to review,</td>
<td>the right to review,</td>
<td>0055:0002</td>
</tr>
<tr>
<td>control, log,</td>
<td>control, log,</td>
<td>control, log,</td>
<td>0065:0017</td>
</tr>
</tbody>
</table>
AUDITS. Law enforcement officials may examine...0058:0056
may utilize the following process for...0074:0012
for business and security purposes to...0002:0020
not serve as official documentation for...0032:0027
& Security staff shall examine firewall...0043:0002
performance of a prospective financial...0033:0005
are subject to periodic inspection or...0005:0011
perform remote hardware and software...0056:0029
Administrators shall configure system...0058:0056
be conducted annually or as required. ...0057:0102
be conducted if Sedgwick...0083:0012
for error correction, forensic...0002:0049
incident is detected through such...0033:0001
11. All users are subject to...0010:0018
perform remote hardware and software...0005:0056
Audits will be conducted with using an...0042:0017
Auditors shall configure system...0044:0009
Count is committed to routinely...0033:0002
compliance through periodic security...0047:0012
Periodical...0008:0056
be conducted annually or as required. ...0033:0016
3 fiscal years provided applicable...0008:0059
department will conduct periodic...0065:0059
be responsible for conducting routine...0034:0047
for access to these resources to...0007:0007
Integrity -Mechanism to...0032:0538
5. The Security Officer shall...0042:0059
* If possible, should use Radius to...0008:0101
or more passwords in order to login and...0069:0132
they are merely a way to identify and...0005:0051
C.2.a. Filters and...0045:0002
network including, but not limited to,...0083:0021
Second, encryption allows for "...0003:0400
re-enter the password (and/or other...0042:0045
" Should support...0002:0217
are used with a password to establish...0007:0107
11. Circumventing user...0005:0034
Sedgwick County shall adopt a message...0006:0047
d) the existence and location of...0058:0048
16.3.7 BACK-UP On-Call Technician...0039:0042
Data...0094:0020
10.5.2 Primary On-Call Technician and...0094:0020
including incremental and full...0037:0014
includes, but is not limited to, the...0083:0020
2.3.2 BACKGROUND...0002:043
Resources will then perform a Criminal...0104:0010
of legal documents, notes, reports,...0068:0000
deploy and which can occur in the...0003:0047
laws and be aware that screen savers,...0053:0021
3.3 Data Storage and BACKUPS .........................................................

The Customer Support Office is the BACKUP triage support location for the Help...

- Monday through Thursday - Incremental BACKUPS, with two-week retention period...

and messages are not included in system to establish the frequency on which noted above; make additional, separate include removing off site tape or disk data should be backed up, and the one cards ____, cell phone ____, BEEPER ____,

social engineering attempts, abnormal Section 2 for more detail), abnormal In addition, if a particular any suspicious, abnormal or unnatural computer user must adopt operating???Gaming: BETTING, gambling, wagering ...

Use technology resources for wagering, All employees, as part of new hire and not indirectly affect the agency; i.e., or grant applicants, contractors or Coordinates the CAPITAL IMPROVEMENT SUCCESSFUL the development of specifications for the development of specifications for - Equipment for handling benefits; marriage, death, divorce and not use family member names, pet names, leave during a year's time for the family member names, favorite hobbies; * The password shall not be your Commonly used words, names, initials, birthdays of equipment, systems or persons, virus...

- BACKUPTAPE; BACKUP SYSTEM BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKUP BACKU
Subject: Business Associates

1. The County email systems for high-volume mail, voice-mail, World Wide Web, new fishing rod and spends over an hour
   PERSONAL USE: Non-business research and network access points, fire and
   Head, to be addressing official
   individuals for facilitation of County
   needs arising in the normal course of
   for the purpose of conducting city
   create or receive in doing the public’s
   for the purpose of conducting city
   access to computer resources including
   residents demand, while applying sound
   residents demand, while applying sound
   ongoing compliance monitoring of all
   ongoing compliance monitoring of all
   and any applicable policies and
   must be justified by a strong
   Quality Assurance of
   D. Within 2
   around* all requests within four (4)
   activity, and use for a personal
   Columbia County IT department for an 8
   to have Planned Downtime during regular
   Support Outside of Regular
   7.3. Calls handled outside of normal
   C.1. Access Required to Conduct County
   user group representative. A legitimate
   Restrict access to cardholder data by
   of employees in satisfying legitimate
   is intended to facilitate County
   are intended to facilitate County
   reference to managing the interests and
   reference to managing the interests and
   reference to managing the interests and
   reference to managing the interests and
   minimize the impact of such auditing on
   consequences. Downtime during general
   (equipment) to support its
   to conduct office of the Chief of New Britain
   to our citizens, County teammates, and
   as necessary in light of changes to
   will not become obsolete and that basic
   property intended for official Town
   use workstations for Sedgwick County’s
   Water District and should be used for
   and ever-changing service demands and
   and uses it to support Village
   is provided for use for County
   to have separate cell phones for
   provided to employees are for official
   and be used for business related purposes.
   property intended for official Town
   enhancements may be authorized.
   enhancements may be authorized.
   products, Dreamweaver, Formium, Adobe002:0300
   such as Internet Explorer
   have all the recommended patches.
   , and FTP, all of which are the property
   BROWSER, File Transfer Protocol, networking and
   BURGLARY alarm equipment, and storage for
   BROWSER applications, electronic mail, and the
   BROWSER approaches associated with:
   BROWSER associate agreements.
   BROWSER associate agreements.
   Associate agreements. Upon return to
   Associates
   case or operational necessity and must
   Critical Information
   days of the new equipment arriving.
   days of receiving them. Media requests.
   enterprise. Use care not to divulge
   hour period. Eight business hour notice
   hours, namely if outside personnel are
   business hours.
   : If the appropriate authorizing
   need must be demonstrated to obtain
   needs of the City.
   objectives for employees and other
   objectives for employees and other
   the County under Public Act 156 of
   the County under Public Act 156 of
   of the County under Public Act 156 of
   operations and to minimize access to
   operations is unacceptable. However,
   operations. Any personal use of these
   or to gain technical expertise
   partners.
   practices and technological
   productivity software can be supported
   purposes, and are not to be used for
   purposes. Highly limited, reasonable
   requirements of County agencies.
   thereby grants to the Village a
   transactions, research, records, and
   use and for personal use. Therefore,
   use, and shall be subject to access by.
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>an agency in connection with official</td>
<td>BUSINESS</td>
<td>which are used to perpetuate</td>
<td>0008:0040</td>
</tr>
<tr>
<td>at the main entryway ONLY to discuss</td>
<td>BUSINESS</td>
<td>with Data Center staff. Going beyond</td>
<td>0049:0029</td>
</tr>
<tr>
<td>an effort to provide a comfortable but</td>
<td>BUSINESS-LIKE</td>
<td>environment for 'Dress Down Friday'</td>
<td>0100:0001</td>
</tr>
<tr>
<td>of public records in a systematic,</td>
<td>BUSINESS-LIKE</td>
<td>manner.</td>
<td>0057:0014</td>
</tr>
<tr>
<td>unless there exists a legitimate</td>
<td>BUSINESS-RELATED</td>
<td>need.</td>
<td>0090:0131</td>
</tr>
<tr>
<td>2. Require all persons not engaged in</td>
<td>BUSINESS-RELATED</td>
<td>activity to leave the Data Center</td>
<td>0049:0091</td>
</tr>
<tr>
<td>employees for any purposes other than</td>
<td>BUSINESS’S</td>
<td>needs. The City of New Britain’s</td>
<td>0061:0023</td>
</tr>
<tr>
<td>that content is in compliance with the</td>
<td>BUSINESSSES</td>
<td>established policies.</td>
<td>0003:0154</td>
</tr>
<tr>
<td>other governments, universities,</td>
<td>BUSINESSSES</td>
<td>, companies, corporations,</td>
<td>0027:0029</td>
</tr>
<tr>
<td>shall not sell programs to firms,</td>
<td>BUSINESSSES</td>
<td>, and individuals for facilitation of</td>
<td>0065:0023</td>
</tr>
<tr>
<td>systems to set up personal</td>
<td>BUSINESSSES</td>
<td>and departments in large enterprises</td>
<td>0092:0009</td>
</tr>
<tr>
<td>agencies, community groups, and</td>
<td>BUSINESSSES</td>
<td>and/or the purchase of systems from</td>
<td>0090:0215</td>
</tr>
<tr>
<td>a midrange server designed for small</td>
<td>BUSINESSES</td>
<td>it is located on the County Intranet site</td>
<td>0003:0393</td>
</tr>
<tr>
<td>rental or loaner systems from local</td>
<td>BUSINESSES</td>
<td>in Schaumburg,</td>
<td>0031:0008</td>
</tr>
<tr>
<td>provides services to residents or</td>
<td>BUSINESSES</td>
<td>files on computer and memory</td>
<td>0032:0029</td>
</tr>
<tr>
<td>with a Clear Building. A link to the training</td>
<td>CALENDAR</td>
<td>month in which the bill copy is</td>
<td>0002:1033</td>
</tr>
<tr>
<td>and will be made by the end of the</td>
<td>CALENDAR</td>
<td>with a reminder that will prompt the</td>
<td>0095:0026</td>
</tr>
<tr>
<td>customer in his/her Microsoft Outlook</td>
<td>CALENDAR</td>
<td>year (i.e. 2002, 2003, etc.).</td>
<td>0008:0044</td>
</tr>
<tr>
<td>for each department will be named the</td>
<td>CALENDAR</td>
<td>All of</td>
<td>0002:0287</td>
</tr>
<tr>
<td>provides remote access to e-mail and</td>
<td>CALENDAR</td>
<td>through an Internet connection.</td>
<td>0065:0049</td>
</tr>
<tr>
<td>computer desktop such as spreadsheets,</td>
<td>CALENDARS</td>
<td>notes, e-mail, etc.</td>
<td>0065:0012</td>
</tr>
<tr>
<td>(Financial and Human Resources System),</td>
<td>CAMA</td>
<td>(Computer Aided Mass Appraisal System:</td>
<td>0003:0328</td>
</tr>
<tr>
<td>3. TV</td>
<td>CAMERA</td>
<td>monitoring of the exits</td>
<td>0049:0082</td>
</tr>
<tr>
<td>* Surveillance</td>
<td>CAMERAS</td>
<td>, alarms, motion detectors</td>
<td>0002:0312</td>
</tr>
<tr>
<td>includes handheld computing devices,</td>
<td>CAMERAS</td>
<td>and other small items in the computer</td>
<td>0009:0111</td>
</tr>
<tr>
<td>but not limited to PDAs, USB drives,</td>
<td>CAMERAS</td>
<td>and phones shall be connected to a</td>
<td>0009:0136</td>
</tr>
<tr>
<td>the agent/sponsor (ie annual United Way</td>
<td>CAMPAIGN</td>
<td>). Prior approval must be obtained to</td>
<td>0010:0006</td>
</tr>
<tr>
<td>prohibited are political activity and</td>
<td>CAPRIS</td>
<td>are acceptable in the office. Pants</td>
<td>0010:0017</td>
</tr>
<tr>
<td>* Slacks, jeans, gauchos and</td>
<td>CARD</td>
<td>The cards are NOT to be loaned or</td>
<td>0049:0012</td>
</tr>
<tr>
<td>access to the Data Center by use of</td>
<td>CARD</td>
<td>fuel authorization____, gate</td>
<td>0106:0009</td>
</tr>
<tr>
<td>the County credit</td>
<td>CARD</td>
<td>and returning it to the software</td>
<td>0058:0048</td>
</tr>
<tr>
<td>for completing the registration</td>
<td>CARD</td>
<td>Industry Approved Scanning Vendors</td>
<td>0065:0004</td>
</tr>
<tr>
<td>Scans must be performed by Payment</td>
<td>CARD</td>
<td>information, confidential tag</td>
<td>0008:0627</td>
</tr>
<tr>
<td>the associated components (e.g., rooms,</td>
<td>CARD</td>
<td>reader controls, etc.)</td>
<td>0034:0036</td>
</tr>
<tr>
<td>a firewall configuration to protect</td>
<td>CARDHOLDER</td>
<td>data</td>
<td>0056:0007</td>
</tr>
<tr>
<td>purchased through user corporate credit</td>
<td>CARDS</td>
<td>, petty cash, and travel or</td>
<td>0058:0046</td>
</tr>
<tr>
<td>The data may include survey response</td>
<td>CARDS</td>
<td>, the results of telephone polls, tally</td>
<td>0008:0334</td>
</tr>
<tr>
<td>determine what keys, tokens, and/or</td>
<td>CARDS</td>
<td>(if any) shall be furnished to persons</td>
<td>0034:0016</td>
</tr>
<tr>
<td>lock, swipe badges, proximity</td>
<td>CARDS</td>
<td>(if any) shall be furnished to individuals</td>
<td>0039:0050</td>
</tr>
<tr>
<td>etc. and County identification</td>
<td>CARDS</td>
<td>and health insurance cards (if</td>
<td>0106:0003</td>
</tr>
<tr>
<td>wireless adaptors will be available. If</td>
<td>CARDS</td>
<td>are not returned in approved amount of</td>
<td>0101:0012</td>
</tr>
<tr>
<td>those individuals assigned proximity</td>
<td>CARDS</td>
<td>which allow controlled access to the</td>
<td>0409:0149</td>
</tr>
<tr>
<td>priority one cards ____., (EMS, Sheriff and Emergency Services),</td>
<td>CELL</td>
<td>phone</td>
<td>0106:0008</td>
</tr>
<tr>
<td>2.7</td>
<td>CELL</td>
<td>phone and pager numbers have been</td>
<td>0003:0366</td>
</tr>
<tr>
<td>the office or primary work location. As</td>
<td>CELL</td>
<td>Phone Use</td>
<td>0002:0112</td>
</tr>
<tr>
<td>Manager's Office for purchase via the fees to a health club/gym, theme park, the policy of Gaston County to provide</td>
<td>CELL</td>
<td>phones are becoming a preferred method</td>
<td>0011:0003</td>
</tr>
<tr>
<td>commercial recycling, documented by a</td>
<td>CELL</td>
<td>phone administrative protocol. Upon</td>
<td>0042:0055</td>
</tr>
<tr>
<td>Record copy. 15 years after issuance of marriage, death, divorce and birth shall generate encryption keys and/or</td>
<td>CELL</td>
<td>phone services, etc., employee____</td>
<td>0010:0006</td>
</tr>
<tr>
<td>Employee</td>
<td>CELL</td>
<td>Telephones</td>
<td>0011:0001</td>
</tr>
<tr>
<td>Do they know anyone involved?</td>
<td>CERTIFICATE</td>
<td>of destruction obtained from the</td>
<td>0057:0108</td>
</tr>
<tr>
<td>1.5</td>
<td>CERTIFICATE</td>
<td>of occupancy</td>
<td>0008:0425</td>
</tr>
<tr>
<td>network must be owned by the County and</td>
<td>CERTIFICATES</td>
<td>; incoming and outgoing correspondence</td>
<td>0008:0454</td>
</tr>
<tr>
<td></td>
<td>CERTIFICATION</td>
<td>for each pertinent workforce member</td>
<td>0042:0055</td>
</tr>
<tr>
<td></td>
<td>CERTIFICATION</td>
<td>form?</td>
<td>0050:0020</td>
</tr>
<tr>
<td></td>
<td>CERTIFIED</td>
<td>that the computer:</td>
<td>0098:0037</td>
</tr>
<tr>
<td></td>
<td>Information Services</td>
<td>}</td>
<td>0083:0046</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4/7/2008 Page 266 of 296
of, or repurposed, data must be \textit{CERTIFIED} deleted or disks destroyed consistent with the above stipend will be used;...
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet messages are public of this Remote Access is to facilitate</td>
<td>COMMUNICATION and are not private. All communications</td>
<td>and convenience. It is a privilege and..0067.0060</td>
<td></td>
</tr>
<tr>
<td>with nearly instantaneous electronic</td>
<td>COMMUNICATION and Internet access, are Town property..0089.0005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>output devices (printers, plotters, to determine whether the electronic</td>
<td>COMMUNICATION capabilities. This connectivity with..0004.0008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>those records created primarily for the of Health and Human Services. Such using County computer technology or could create the perception that the</td>
<td>COMMUNICATION systems. Because of the need to..0002.0018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>employees, directors will determine if providers, America On-Line, Prodigy, Service Provider accounts (i.e. AOL, 4. If Information Services does not by facsimile or e-mail, is not</td>
<td>COMMUNICATION was made in one's official capacity as.....0091.0096</td>
<td></td>
<td></td>
</tr>
<tr>
<td>by City Computing Resources may be</td>
<td>COMMUNICATION with professional associations, other..0065.0023</td>
<td></td>
<td></td>
</tr>
<tr>
<td>of theft, unauthorized disclosure of</td>
<td>COMMUNICATION with security/police.............................0039.0056</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information: Sending information deemed</td>
<td>CONFIDENTIAL and may be reviewed by others...........0089.0009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individuals accessing</td>
<td>CONFIDENTIAL proprietary information of the county ....0003.0006</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revealing unauthorized or Revealing unauthorized or</td>
<td>CONFIDENTIAL &quot; or &quot;Do Not Forward&quot; when permission.....0001.0025</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I may be provided access to highly from the vendor. Records containing</td>
<td>CONFIDENTIAL and employees are responsible for.........0091.0117</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail should not be used to transmit</td>
<td>CONFIDENTIAL and/or sensitive information are.........0083.0066</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Such reports shall be treated as passbery access to High Risk and is not a secure method for transmitting not gain access to such work-related or</td>
<td>CONFIDENTIAL information in order to perform my job.....0059.0004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>databases or applications which contain that the release of Columbia County that the release of Columbia County</td>
<td>CONFIDENTIAL information may be shredded prior to....0031.0010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1) Although</td>
<td>CONFIDENTIAL information, the loss of data or loss ..0101.0027</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Althrough shall address the importance of investigation will be maintained as</td>
<td>CONFIDENTIAL information, the loss of data or loss......0105.0023</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.0 -</td>
<td>CONFIDENTIAL information without advice from the....0090.0097</td>
<td></td>
<td></td>
</tr>
<tr>
<td>necessary to preserve the integrity, security principles of availability, of employer, employee or customer</td>
<td>CONFIDENTIAL information. Such passwords protected.....0004.0026</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the expected accessibility, integrity,</td>
<td>CONFIDENTIAL passwords are issued, users should be.....0007.0009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. CONFIDENTIALITY ......................0004.0025</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copyright infringement, and so on.</td>
<td>CONFIDENTIALITY, integrity, and availability of e-Phil..0046.0009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>, and availability of its facilities, ......0040.0017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>, and integrity. This policy applies to.....0063.0003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>, copyright infringements, and so on. .....0061.0035</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>, integrity, and availability of e-Phi...........0032.0004</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>, integrity, and availability of the...........0038.0017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>, integrity, and availability of e-Phil...........0059.0011</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>, longevity and recoverability needs and....0083.0052</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
KWIC INDEX TO GMIS POLICIES

<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>c) Caution involved staff about</td>
<td></td>
<td></td>
<td>0050:0021</td>
</tr>
<tr>
<td>according to Town requirements for</td>
<td></td>
<td></td>
<td>0060:0027</td>
</tr>
<tr>
<td>on those systems consistent with its</td>
<td></td>
<td></td>
<td>0068:0044</td>
</tr>
<tr>
<td>BE NO EXPECTATION OF PRIVACY OR</td>
<td></td>
<td></td>
<td>0003:0072</td>
</tr>
<tr>
<td>12.5.3 Protection of</td>
<td></td>
<td></td>
<td>0091:0116</td>
</tr>
<tr>
<td>management cannot guarantee the</td>
<td></td>
<td></td>
<td>0002:0018</td>
</tr>
<tr>
<td>(90) days. This is to protect the</td>
<td></td>
<td></td>
<td>0077:0007</td>
</tr>
<tr>
<td>* Maintains the security and</td>
<td></td>
<td></td>
<td>0069:0025</td>
</tr>
<tr>
<td>data are required to maintain the</td>
<td></td>
<td></td>
<td>0005:0060</td>
</tr>
<tr>
<td>This also ensures the integrity and</td>
<td></td>
<td></td>
<td>0065:0043</td>
</tr>
<tr>
<td>a personalized Network Password. The</td>
<td></td>
<td></td>
<td>0016:0007</td>
</tr>
<tr>
<td>of a voice mail box password/code. The</td>
<td></td>
<td></td>
<td>0029:0018</td>
</tr>
<tr>
<td>shall never use information obtained</td>
<td></td>
<td></td>
<td>0068:0050</td>
</tr>
<tr>
<td>shall never use information obtained</td>
<td></td>
<td></td>
<td>0069:0014</td>
</tr>
<tr>
<td>that breaches the City of New Britain.</td>
<td></td>
<td></td>
<td>0061:0001</td>
</tr>
<tr>
<td>IT staff or local IT staff prior to</td>
<td></td>
<td></td>
<td>0099:0001</td>
</tr>
<tr>
<td>*</td>
<td></td>
<td></td>
<td>0003:0195</td>
</tr>
<tr>
<td>The Internet is a global network</td>
<td></td>
<td></td>
<td>0091:0024</td>
</tr>
<tr>
<td>The Internet is a global network</td>
<td></td>
<td></td>
<td>0092:0104</td>
</tr>
<tr>
<td>IT department will support the user in</td>
<td></td>
<td></td>
<td>0018:0017</td>
</tr>
<tr>
<td>the identity of any outside agency</td>
<td></td>
<td></td>
<td>0067:0025</td>
</tr>
<tr>
<td>and calendaring through an Internet</td>
<td></td>
<td></td>
<td>0062:0034</td>
</tr>
<tr>
<td>A secure, encrypted remote access</td>
<td></td>
<td></td>
<td>0065:0049</td>
</tr>
<tr>
<td>County's network, Internet and e-mail installation of hardware to support the</td>
<td></td>
<td></td>
<td>0066:0020</td>
</tr>
<tr>
<td>peripheral, software, and network</td>
<td></td>
<td></td>
<td>0003:0074</td>
</tr>
<tr>
<td>The Town has limited bandwidth in its</td>
<td></td>
<td></td>
<td>0068:0018</td>
</tr>
<tr>
<td>a &quot;fast resort&quot; and used only when a</td>
<td></td>
<td></td>
<td>0020:0003</td>
</tr>
<tr>
<td>made or received by an agency in their</td>
<td></td>
<td></td>
<td>0066:0014</td>
</tr>
<tr>
<td>their government e-mail addresses in</td>
<td></td>
<td></td>
<td>0008:0040</td>
</tr>
<tr>
<td>materials neither made nor received in</td>
<td></td>
<td></td>
<td>0090:0101</td>
</tr>
<tr>
<td>e-mails will only be accessed through</td>
<td></td>
<td></td>
<td>0057:0128</td>
</tr>
<tr>
<td>(including virus protection), network</td>
<td></td>
<td></td>
<td>0009:091</td>
</tr>
<tr>
<td>and all existing and future network</td>
<td></td>
<td></td>
<td>0067:0030</td>
</tr>
<tr>
<td>user-ids. All internal and external</td>
<td></td>
<td></td>
<td>0063:0003</td>
</tr>
<tr>
<td>for the departmental work. All</td>
<td></td>
<td></td>
<td>0053:0020</td>
</tr>
<tr>
<td>IPSec Virtual Private Network (VPN)</td>
<td></td>
<td></td>
<td>0050:0046</td>
</tr>
<tr>
<td>only exception will be those existing</td>
<td></td>
<td></td>
<td>0006:0048</td>
</tr>
<tr>
<td>of Commissioners' network via wireless network</td>
<td></td>
<td></td>
<td>0101:0003</td>
</tr>
<tr>
<td>VPN does not provide Internet</td>
<td></td>
<td></td>
<td>0105:0008</td>
</tr>
<tr>
<td>3.a.</td>
<td></td>
<td></td>
<td>0053:0006</td>
</tr>
<tr>
<td>library resources, Internet/Intranet</td>
<td></td>
<td></td>
<td>0091:0016</td>
</tr>
<tr>
<td>library resources, Internet/Intranet</td>
<td></td>
<td></td>
<td>0053:0008</td>
</tr>
<tr>
<td>C. Network</td>
<td></td>
<td></td>
<td>0067:0034</td>
</tr>
<tr>
<td>C.2.c. Additional Costs: Costs for</td>
<td></td>
<td></td>
<td>0064:0011</td>
</tr>
<tr>
<td>3.b.3. To permit limited</td>
<td></td>
<td></td>
<td>0018:0020</td>
</tr>
<tr>
<td>Department reserves the right to remove</td>
<td></td>
<td></td>
<td>0002:0271</td>
</tr>
<tr>
<td>4.1.3 Software and Network</td>
<td></td>
<td></td>
<td>0065:0047</td>
</tr>
<tr>
<td>of Aeronautics may establish user</td>
<td></td>
<td></td>
<td>0065:0048</td>
</tr>
<tr>
<td>communication capabilities. This</td>
<td></td>
<td></td>
<td>0033:0184</td>
</tr>
<tr>
<td>data and systems. The County's network</td>
<td></td>
<td></td>
<td>0027:0031</td>
</tr>
<tr>
<td>own time will not use Village time to</td>
<td></td>
<td></td>
<td>0057:0068</td>
</tr>
<tr>
<td>The Records Manager will</td>
<td></td>
<td></td>
<td>0058:0052</td>
</tr>
<tr>
<td>use software at home, he / she should</td>
<td></td>
<td></td>
<td>0068:0050</td>
</tr>
<tr>
<td>of information varies, employees should</td>
<td></td>
<td></td>
<td>0069:0114</td>
</tr>
<tr>
<td>of information varies, employees should</td>
<td></td>
<td></td>
<td>0008:0334</td>
</tr>
<tr>
<td>of operations. This does not include a</td>
<td></td>
<td></td>
<td>0005:0010</td>
</tr>
<tr>
<td>scanning tool or use of a vendor or</td>
<td></td>
<td></td>
<td>0063:0008</td>
</tr>
<tr>
<td>within the County IT environment, e.g.,</td>
<td></td>
<td></td>
<td>0064:0002</td>
</tr>
<tr>
<td>Remote access required by vendors,</td>
<td></td>
<td></td>
<td>0009:0104</td>
</tr>
<tr>
<td>Remote access required by vendors,</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities may</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
<tr>
<td>CONSULTANTS, and other non-County entities will</td>
<td></td>
<td></td>
<td>0066:0004</td>
</tr>
</tbody>
</table>
3. **CONTRACTORS** are granted access by notifying the ..........0049:0031

4. Policy applies to all employees, independent interns, volunteers, consultants, sections herein apply to employees, is not limited to: software vendors, / software or from clients.

5. **E-mail Systems:**

6. **Facilities or time unless a written license is a**

7. **For completion or termination of unsuccessful, to terminate the**

8. **When employment is terminated, when the connected to specific case files, the computer system and/or have their in formulating a disaster recovery departments will find it beneficial to that pertain to their specific applies to all divisions, departments, individual, or non-DIO/IT employee technical staff which includes vendors, or individuals (third parties) employees who are responsible for the to an individual. No employee or to any County official, employee, shall provide every staff member, For VPN access being provided to a department staff or their designated

9. **employees, and employees working under the using Department, frequently under facilities or time unless a written**

10. **Any Village of Schaumburg employee or CONTRACTOR who develops computer software (or**

11. **Any deviations to the standard service**

12. **Expiration of the current**

13. **to properly execute a standard service employees, and employees working under employees, and employees working under the using Department, frequently under**

14. **policy applies to all County employees, to: software vendors, contractors, other authorized current users such as 5.a. E-mail Systems:**

15. **CONSULTANTS** , and 3rd party vendors who may access...0101:0005

16. **CONSULTANTS** , contractors and temporary staff. ............0005:0074

17. **CONSULTANTS** , contractors and vendors may use their...0062:0018

18. **CONSULTANTS** , internal staff, hardware, software,.....0032:0057

19. **CONSULTANTS** , must be authorized through the Usage...0065:0008

20. **CONSULTANTS** , must be authorized through the Usage...0066:0009

21. **CONSULTANTS** , temporary, and other workers at........0002:0005

22. **CONSULTANTS** and vendors. .........................0048:0007

23. **CONSULTANTS** to develop and maintain security........0047:0008

24. **CONSULTANTS** from the manufacturer. .................0096:0030

25. **CONSULTANTS** in which a party with proper authority .....0058:0025

26. **CONSULTANTS** /lease/agreement provided applicable ..0008:0015

27. **CONSULTANTS** or arrangement. If termination of the........0038:0029

28. **CONSULTANTS** or the Non-union complaint procedure in...0001:0040

29. **CONSULTANTS** (project expires at Martin County...0057:0000

30. **CONSULTANTS** related or otherwise an essential part......0003:0165

31. **CONSULTANTS** revoked. In addition, other legal..........0007:0029

32. **CONSULTANTS** with an outside vendor to achieve.........0015:0011

33. **CONSULTANTS** work. ........................................0005:0020

34. **CONSULTANTS** entities, and other individuals or.......0053:0010

35. **CONSULTANTS** or assigned by the County to perform.....0049:0014

36. **CONSULTANTS** personnel, and information technology.....0065:0021

37. **CONSULTANTS** to do work for the County, or use........0003:0072

38. **CONSULTANTS** and/or supervising of the third party........0003:0272

39. **CONTRACTOR** , etc. may have more than one computer...0006:0016

40. **CONTRACTOR** or other individual approved to access.....0067:0008

41. **CONTRACTOR** , part-time employee, volunteer, or.........0004:0021

42. **CONTRACTOR** , this date cannot be beyond the........0004:0009

43. **CONTRACTOR** (s). The procurement of these items is.......0002:0027

44. **CONTRACTOR** : a company, individual, or non-DIO/IT.....0049:0014

45. **CONTRACTOR** employees as necessary for the..........0091:0007

46. **CONTRACTOR** is working on the server. When ..........0068:0084

47. **CONTRACTOR** or mechanical contractor applies to ........0008:0441

48. **CONTRACTOR** personnel. ...............................0092:0120

49. **CONTRACTOR** who develops employee or of the Bradford County IT staff or any

50. **CONTRACTOR** who will ever ask for your username and....0069:0102

51. **CONTRACTOR**’s staff expected to arrive? ..................0049:0040

52. **CONTRACTORS** , and other computer users. All........0001:0001

53. **CONTRACTORS** , and vendors who access the County’s...0005:0015

54. **CONTRACTORS** , consultants, temporary, and other......0002:0005

55. **CONTRACTORS** , consultants, business partners, and.....0003:0275

56. **CONTRACTORS** , customers and others. ..........................0006:0333

57. **CONTRACTORS** , part-time employees, vendors, and.....0004:0017

58. **CONTRACTORS** , part-time employees, volunteers, and.....0007:0029

59. **CONTRACTORS** , vendors, or others, will be permitted.....0062:0015

60. **CONTRACTORS** , vendors, transfers, and terminations) ....0066:0033

61. **CONTRACTORS** . Approval is the responsibility of ....0083:0048

62. **CONTRACTORS** and temporary staff. Accounts may be...0005:0074

63. **CONTRACTORS** are granted access by notifying the........0049:0031

64. **CONTRACTORS** may attach network devices to the.......0069:0037

65. **CONTRACTORS** of the Division of.........................0053:0025

66. **CONTRACTORS** . part of a record, or business............0089:0016
cell phones, or enter into cell phone CONTRACTS, to be used by employees for business.....0011:0003

created and managed according to CONTRACTS and Procurement policy and Information.....0083:0036

to the FLAGG Committee on the award of CONTRACTS for bids on replacement equipment........0023:0062

to the FLAGG Committee on the award of CONTRACTS for bids on replacement equipment........0025:0061

and external programming resources. All CONTRACTS for custom software will include..........0015:0003

approved by the Legal Department. All CONTRACTS require Board of County Commissioners ..0051:0070

system privileges and/or have their CONTRACTS revoked. Additional legal remedies may ....0004:0043

usage privileges and/or have their CONTRACTS revoked. Additional legal remedies may ....0005:0129

Charleston County CONTRACTS with PST, Inc. to provide training ..............0039:0393

Memorandum of Agreement (MOA) or other CONTRACTUAL arrangement.................0063:0008

* Because cell phone service is a CONTRACTUAL agreement between the cell phone........0011:0033

is noncommercial in nature and/or has a CONTRACTUAL agreement for the use of Village of.......0031:0010

hardware, etc., unless there is a CONTRACTUAL agreement with the Village allowing........0027:0033

a relationship requires identifying CONTRACTUAL agreements and maintaining a close ........0002:0377

Memorandum of Agreement (MOA) or other CONTRACTUAL association.................0063:0008

SUBJECT: Facility Access SUBJECT: Device and Media SUBJECT: Access SUBJECT: Audit

SUBJECT: Transmission Security components (e.g., rooms, card reader * Maintains and

and ensure all applicable access identify the various security

1. See policy entitled Audit software by enforcing strong internal

www.branford-ct.gov as the “home page”. F.7.b. Violation of

of any person or company protected by penalties under the United States provided to programs and data by

Computer Software Policy to enforce compliance with software licensing and

To protect against the possibility of in downloading software. Adhere to

Internet may be protected by federal

Copyright Policy ................................. ......................0069:0046

COPYRIGHT ................................................... ........0046:0002

COPYRIGHT ................................................... ........0043:0002

COPYRIGHT ................................................... ........0041:0002

COPYRIGHT ................................................... ........0040:0002

COPYRIGHT ................................................... ........0039:0003

COPYRIGHT ................................................... ........0038:0002

COPYRIGHT ................................................... ........0037:0019

COPYRIGHT ................................................... ........0036:0018

COPYRIGHT ................................................... ........0035:0017

COPYRIGHT ................................................... ........0034:0016

COPYRIGHT ................................................... ........0033:0015

COPYRIGHT ................................................... ........0032:0014

COPYRIGHT ................................................... ........0031:0013

COPYRIGHT ................................................... ........0030:0012

COPYRIGHT ................................................... ........0029:0011

COPYRIGHT ................................................... ........0028:0010

COPYRIGHT ................................................... ........0027:0009

COPYRIGHT ................................................... ........0026:0008

COPYRIGHT ................................................... ........0025:0007

COPYRIGHT ................................................... ........0024:0006

COPYRIGHT ................................................... ........0023:0005

COPYRIGHT ................................................... ........0022:0004

COPYRIGHT ................................................... ........0021:0003

COPYRIGHT ................................................... ........0020:0002

COPYRIGHT ................................................... ........0019:0001

COPYRIGHT ................................................... ........0018:0000

COPYRIGHT ................................................... ........0017:0009

COPYRIGHT ................................................... ........0016:0017

COPYRIGHT ................................................... ........0015:0016

COPYRIGHT ................................................... ........0014:0015

COPYRIGHT ................................................... ........0013:0014

COPYRIGHT ................................................... ........0012:0013

COPYRIGHT ................................................... ........0011:0012

COPYRIGHT ................................................... ........0010:0011

COPYRIGHT ................................................... ........0009:0010

COPYRIGHT ................................................... ........0008:0009

COPYRIGHT ................................................... ........0007:0008

COPYRIGHT ................................................... ........0006:0007

COPYRIGHT ................................................... ........0005:0006

COPYRIGHT ................................................... ........0004:0005

COPYRIGHT ................................................... ........0003:0004

COPYRIGHT ................................................... ........0002:0003

COPYRIGHT ................................................... ........0001:0002

COPYRIGHT ................................................... ........0000:0001
and determine the most effective, and
determines the most effective, and by using
appear to be from an authorized source (hazards, vulnerabilities, and/or
mail is an option for the customer as a
Employees are expected to demonstrate manager for dissemination. A
(such communications may also be a
User has committed, or is committing a
course of an ongoing investigation of
Human Resources will then perform a
as being subject to Kansas civil and
in personal liability, civil and / or
/or Sedgwick County to both civil and
which may include termination and/or
E-mail system may be referred for
the computer system may be referred for
adult/sexually explicit, violence,

The easiest way for

Delegation of the necessary authority
CUSTODIAL

and must ensure that the data
3. The appropriate
is reasonably necessary to allow the
" Data
County divisions / departments are the
administration (VA) benefits; marriage, DEATH, divorce and birth certificates;

a. High (3) -

whose failure may cause injury or
" Disk

are from replacement charges (funded
are from replacement charges (funded
may also be subject to Kansas civil and
which may include termination and/or
E-mail system may be referred for
the computer system may be referred for
adult/sexually explicit, violence,

The easiest way for

Delegation of the necessary authority
CUSTODIAL

and must ensure that the data
3. The appropriate
is reasonably necessary to allow the
" Data
County divisions / departments are the
administration (VA) benefits; marriage, DEATH, divorce and birth certificates;

a. High (3) -

whose failure may cause injury or
" Disk

are from replacement charges (funded
are from replacement charges (funded
may also be subject to Kansas civil and
which may include termination and/or
E-mail system may be referred for
the computer system may be referred for
adult/sexually explicit, violence,

The easiest way for

Delegation of the necessary authority
CUSTODIAL

and must ensure that the data
3. The appropriate
is reasonably necessary to allow the
" Data
County divisions / departments are the
administration (VA) benefits; marriage, DEATH, divorce and birth certificates;

a. High (3) -

whose failure may cause injury or
" Disk

are from replacement charges (funded
are from replacement charges (funded
may also be subject to Kansas civil and
which may include termination and/or
E-mail system may be referred for
the computer system may be referred for
adult/sexually explicit, violence,
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>political beliefs, national origin, or</td>
<td>DISABILITY</td>
<td>..........................</td>
<td>0060:0051</td>
</tr>
<tr>
<td>age, sexual preference or handicap or</td>
<td>DISABILITY</td>
<td>. Harassment is broadly defined as..........</td>
<td>0069:0199</td>
</tr>
<tr>
<td>national origin, sexual orientation or</td>
<td>DISABILITY</td>
<td>. Indecent, vulgar, harassing,.............</td>
<td>0089:0008</td>
</tr>
<tr>
<td>creed, national origin, age, or</td>
<td>DISCLAIMER</td>
<td>: Information Technology does not..........</td>
<td>0103:0016</td>
</tr>
<tr>
<td>behalf of Butler County, the following</td>
<td>DISCLAIMER</td>
<td>must be added to all communications:........</td>
<td>0090:0116</td>
</tr>
<tr>
<td>County policy, therefore the following</td>
<td>DISCLAIMER</td>
<td>should be attached to all E-mail..........</td>
<td>0004:0018</td>
</tr>
<tr>
<td>address to newsgroups must contain a</td>
<td>DISCLAIMER</td>
<td>stating that the opinions expressed are....</td>
<td>0005:0017</td>
</tr>
<tr>
<td>Customer Support Center (helpdesk) upon</td>
<td>DISCOVERY</td>
<td>.........................</td>
<td>0053:0021</td>
</tr>
<tr>
<td>confiscation and/or deletion upon</td>
<td>DISCOVERY</td>
<td>.........................</td>
<td>0065:0037</td>
</tr>
<tr>
<td>system performance and integrity, any</td>
<td>DISCOVERY</td>
<td>of abuse by network security staff will.....</td>
<td>0002:0254</td>
</tr>
<tr>
<td>corrective action in the event of</td>
<td>DISCOVERY</td>
<td>of the existence of a computer virus.......</td>
<td>0068:0322</td>
</tr>
<tr>
<td>hate groups, pornographic material or</td>
<td>DISCRIMINATE</td>
<td>against people because of their.............</td>
<td>0002:0085</td>
</tr>
<tr>
<td>explicit materials, obscene and</td>
<td>DISCRIMINATORY</td>
<td>language or solicitation for commercial....</td>
<td>0090:0100</td>
</tr>
<tr>
<td>religious, threatening and/or</td>
<td>DISCRIMINATORY</td>
<td>remarks. Receipt of objectionable.........</td>
<td>0065:0029</td>
</tr>
<tr>
<td>offensive, harassing, demeaning, or</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0082:0135</td>
</tr>
<tr>
<td>DISRUPTIVE to any member of the workforce. Such</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0032:0466</td>
</tr>
<tr>
<td>to be used to create any offensive or</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0041:0013</td>
</tr>
<tr>
<td>DISRUPTIVE messages. Among those which are....</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0008:0680</td>
</tr>
<tr>
<td>for the creation or distribution of any</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0055:0038</td>
</tr>
<tr>
<td>offensive, harassing, demeaning, or</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0057:0008</td>
</tr>
<tr>
<td>from the productivity of others, DISRUPTS network usage, and ties up resources.</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0068:0188</td>
</tr>
<tr>
<td>due to tampering, vandalism or equally</td>
<td>DISPOSAL</td>
<td>of eligible records.........................</td>
<td>0007:0051</td>
</tr>
<tr>
<td>DISTURBING phenomenon. All departments utilizing</td>
<td>DISPOSAL</td>
<td>.........................</td>
<td>0003:0134</td>
</tr>
<tr>
<td>effects security breaches or distribute, upload or download any</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0008:0019</td>
</tr>
<tr>
<td>8. Use the network to</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0057:0039</td>
</tr>
<tr>
<td>Use of the Internet must not</td>
<td>DISRUPT</td>
<td>form the final action for records.............</td>
<td>0007:0051</td>
</tr>
<tr>
<td>access of a host if that host is</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0066:0033</td>
</tr>
<tr>
<td>duties. For purposes of this section, &quot;</td>
<td>DISRUPT</td>
<td>of files. Department Directors will........</td>
<td>0004:0045</td>
</tr>
<tr>
<td>product repairs and reduce work</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0069:0225</td>
</tr>
<tr>
<td>could cause congestion, delay, or</td>
<td>DISRUPT</td>
<td>schedules approved by the County............</td>
<td>0008:0030</td>
</tr>
<tr>
<td>to User PCs and where there may be a</td>
<td>DISRUPT</td>
<td>...............</td>
<td>0003:0129</td>
</tr>
<tr>
<td>seamlessly, minimize application</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0011:0077</td>
</tr>
<tr>
<td>network Users, services or equipment.</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0061:0007</td>
</tr>
<tr>
<td>8. Effecting security breaches or distribute, upload or download any</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0065:0011</td>
</tr>
<tr>
<td>Create, access or transmit any obscene,</td>
<td>DISRUPT</td>
<td>...............</td>
<td>0003:0129</td>
</tr>
<tr>
<td>to be used to create any offensive or</td>
<td>DISRUPT</td>
<td>of network communication. Security........</td>
<td>0005:0031</td>
</tr>
<tr>
<td>for the creation or distribution of any</td>
<td>DISRUPT</td>
<td>, abusive, harassing, threatening, or........</td>
<td>0003:0123</td>
</tr>
<tr>
<td>offensive, harassing, demeaning, or</td>
<td>DISRUPT</td>
<td>, slanderer, defamatory, derogatory or.......</td>
<td>0004:0034</td>
</tr>
<tr>
<td>from the productivity of others,</td>
<td>DISRUPT</td>
<td>of offensive messages, including.............</td>
<td>0006:0051</td>
</tr>
<tr>
<td>due to tampering, vandalism or equally</td>
<td>DISRUPT</td>
<td>to any member of the workforce. Such........</td>
<td>0040:0023</td>
</tr>
<tr>
<td>plan), meeting minutes from LPA and</td>
<td>DISRUPT</td>
<td>network usage, and ties up resources........</td>
<td>0006:0030</td>
</tr>
<tr>
<td>such as but not limited to HIPAA,</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0026:0003</td>
</tr>
<tr>
<td>that are either sexually explicit, have</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0002:0296</td>
</tr>
<tr>
<td>records are subject to audit by the</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0008:0566</td>
</tr>
<tr>
<td>upon a pre-employment physical and</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0068:0038</td>
</tr>
<tr>
<td>to be revived, by the administration of</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0003:0241</td>
</tr>
<tr>
<td>dating, glamour and intimate apparel,</td>
<td>DISRUPT</td>
<td>of Enforcement Administration. Some.........</td>
<td>0008:0461</td>
</tr>
<tr>
<td>service via dial-up, cable modem,</td>
<td>DISRUPT</td>
<td>screen. A phone call followed by a........</td>
<td>0104:0012</td>
</tr>
<tr>
<td>standards for office automation and</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0082:0019</td>
</tr>
<tr>
<td>e-workers better able to provide</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0008:0608</td>
</tr>
<tr>
<td>&quot;Enable Web-Based such as spreadsheets, calendars, notes,</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0006:0007</td>
</tr>
<tr>
<td>and Alcohol, and CYS are in this class........</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0105:0008</td>
</tr>
<tr>
<td>DRUG and alcohol, remote proxies........</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0065:0013</td>
</tr>
<tr>
<td>DRUG, Alcohol, &amp; Tobacco ..................</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0082:0019</td>
</tr>
<tr>
<td>DRUG, both intercardiac and intravenously,........</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0006:0013</td>
</tr>
<tr>
<td>DRUGS and alcohol, hacking, remote proxies........</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0008:0030</td>
</tr>
<tr>
<td>DRUGS, E-GOVERNMENT applications are presented in the table........</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0002:0272</td>
</tr>
<tr>
<td>DSL or other means in order to use........</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0065:0007</td>
</tr>
<tr>
<td>E-GOVERNMENT services.......................</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0053:0007</td>
</tr>
<tr>
<td>when appropriate............................</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0090:0012</td>
</tr>
<tr>
<td>DRUGS, E-GOVERNMENT when appropriate........</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0065:0012</td>
</tr>
<tr>
<td>E-MAIL, etc................................</td>
<td>DISRUPT</td>
<td>.........................</td>
<td>0082:0028</td>
</tr>
<tr>
<td>LEFT CONTEXT</td>
<td>KEYWORD</td>
<td>RIGHT CONTEXT</td>
<td>DOC:LINE</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>with applications, the user may call, the computer system, including employee</td>
<td>E-MAIL</td>
<td>, or visit the applicable application</td>
<td>0014:0006</td>
</tr>
<tr>
<td>The Town's system, including</td>
<td>E-MAIL</td>
<td>, voice mail, facsimile communication</td>
<td>0089:0005</td>
</tr>
<tr>
<td>and external networks, electronic mail (</td>
<td>E-MAIL</td>
<td>), Internet, modems, and facsimile</td>
<td>0068:0007</td>
</tr>
<tr>
<td>involving electronic-mail (</td>
<td>E-MAIL</td>
<td>) provided to employees for use in</td>
<td>0071:0003</td>
</tr>
<tr>
<td>of Internet access and Electronic Mail (</td>
<td>E-MAIL</td>
<td>) that replace written / faxed</td>
<td>0057:0134</td>
</tr>
<tr>
<td>electronic mail communications (</td>
<td>E-MAIL</td>
<td>&amp; Internet</td>
<td>0060:0001</td>
</tr>
<tr>
<td>Policy for Use of Computers,</td>
<td>E-MAIL</td>
<td>Acceptable Use Policy</td>
<td>0004:0001</td>
</tr>
<tr>
<td>duties as stated in the County's</td>
<td>E-MAIL</td>
<td>Acceptable Use Policy</td>
<td>007:0026</td>
</tr>
<tr>
<td>Computer System can be found in the</td>
<td>E-MAIL</td>
<td>address. By doing this, you will limit</td>
<td>0053:0013</td>
</tr>
<tr>
<td>the organization who know your County</td>
<td>E-MAIL</td>
<td>addresses for all persons to be</td>
<td>0037:0051</td>
</tr>
<tr>
<td>f. Telephone numbers and/or</td>
<td>E-MAIL</td>
<td>and Internet access must be submitted</td>
<td>0077:0006</td>
</tr>
<tr>
<td>ID will not be issued. All requests for</td>
<td>E-MAIL</td>
<td>may be subject to disclosure pursuant</td>
<td>0002:0018</td>
</tr>
<tr>
<td>County systems, which include</td>
<td>E-MAIL</td>
<td>messages, discussions during staff</td>
<td>0035:0023</td>
</tr>
<tr>
<td>directory services, DHCP, DNS,</td>
<td>E-MAIL</td>
<td>messages with short-lived, or no</td>
<td>0008:0031</td>
</tr>
<tr>
<td>E-mail-By far, most viruses are sent as</td>
<td>E-MAIL</td>
<td></td>
<td>0040:0019</td>
</tr>
<tr>
<td>internet files or deleted and sent</td>
<td>E-MAIL</td>
<td>clients other than Microsoft Outlook</td>
<td>0092:0239</td>
</tr>
<tr>
<td>directors will be advised via</td>
<td>E-MAIL</td>
<td>if any personnel are affected. Unless</td>
<td>0067:0042</td>
</tr>
<tr>
<td>stored on County technology or sent via</td>
<td>E-MAIL</td>
<td>may be subject to disclosure pursuant</td>
<td>0002:0018</td>
</tr>
<tr>
<td>such reminders through formal training</td>
<td>E-MAIL</td>
<td>messages. discusions during staff</td>
<td>0035:0023</td>
</tr>
<tr>
<td>would include, but are not limited to:</td>
<td>E-MAIL</td>
<td>messages</td>
<td>0008:0031</td>
</tr>
<tr>
<td>of computer files and drives</td>
<td>E-MAIL</td>
<td>Policy</td>
<td>0010:0001</td>
</tr>
<tr>
<td>&quot;all_martin&quot;</td>
<td>E-MAIL</td>
<td>Policy</td>
<td>0061:0001</td>
</tr>
<tr>
<td>will be done in person, by phone or</td>
<td>E-MAIL</td>
<td>request from Courthouse Security or</td>
<td>0049:0089</td>
</tr>
<tr>
<td>office productivity suite software and</td>
<td>E-MAIL</td>
<td>systems have lead to the inability to</td>
<td>0090:0023</td>
</tr>
<tr>
<td>and use of the network, Internet and/or</td>
<td>E-MAIL</td>
<td>systems is provided to employees of</td>
<td>0003:0072</td>
</tr>
<tr>
<td>To ban the use of external Web Based</td>
<td>E-MAIL</td>
<td>Systems in order to protect the</td>
<td>0079:0002</td>
</tr>
<tr>
<td>on a non-secure media or be sent by</td>
<td>E-EMAIL</td>
<td>unless encrypted. It should not be</td>
<td>0072:0004</td>
</tr>
<tr>
<td>*</td>
<td>E-MAIL-BY</td>
<td>far, most viruses are sent as e-mail</td>
<td>0076:0010</td>
</tr>
<tr>
<td>state and federal laws. All data,</td>
<td>E-MAILS</td>
<td>, e-mail attachments, documents and</td>
<td>0003:0072</td>
</tr>
<tr>
<td>should not attempt to send or receive</td>
<td>E-MAILS</td>
<td>, open new programs, or reboot</td>
<td>0040:0033</td>
</tr>
<tr>
<td>&quot;all_martin&quot;</td>
<td>E-MAILS</td>
<td>are sent to advise all Martin County</td>
<td>0010:0006</td>
</tr>
<tr>
<td>e-mail and is able to re-create</td>
<td>E-MAILS</td>
<td>even if both sender and reader have</td>
<td>0050:0096</td>
</tr>
<tr>
<td>city communications. Please note, that</td>
<td>E-MAILS</td>
<td>may be subject to disclosure pursuant</td>
<td>0071:0012</td>
</tr>
<tr>
<td>Due to confidentiality of information,</td>
<td>E-MAILS</td>
<td>will only be accessed through</td>
<td>0069:0091</td>
</tr>
<tr>
<td>changes impacting the security of</td>
<td>E-MAILS</td>
<td>, e.g., addition of new hardware or</td>
<td>0035:0018</td>
</tr>
<tr>
<td>information systems that contain or use</td>
<td>E-MAILS</td>
<td>Policy</td>
<td>0033:0013</td>
</tr>
<tr>
<td>that damages systems that contain</td>
<td>E-MAILS</td>
<td></td>
<td>0037:0006</td>
</tr>
<tr>
<td>or class of workstation that can access</td>
<td>E-MAILS</td>
<td>The policy also identifies physical</td>
<td>0040:0005</td>
</tr>
<tr>
<td>or other means of controlled access to</td>
<td>E-MAILS</td>
<td>; lost access badge; unauthorized</td>
<td>0036:0013</td>
</tr>
<tr>
<td>protected health information (&quot;</td>
<td>E-MAILS</td>
<td>&quot;).</td>
<td>0042:0005</td>
</tr>
<tr>
<td>purpose of this policy is to protect</td>
<td>E-MAILS</td>
<td>&quot;).</td>
<td>0043:0005</td>
</tr>
<tr>
<td>Sedgwick County authorizes access to</td>
<td>E-MAILS</td>
<td>as it is received into and removed from</td>
<td>0041:0005</td>
</tr>
<tr>
<td>policy is to protect Sedgwick County's</td>
<td>E-EMAIL</td>
<td>for its workforce members in a manner</td>
<td>0034:0006</td>
</tr>
<tr>
<td>integrity, and availability of</td>
<td>E-EMAIL</td>
<td>from improper alteration or</td>
<td>0044:0005</td>
</tr>
<tr>
<td>to ensure that Sedgwick County's</td>
<td>E-EMAIL</td>
<td>held by Sedgwick County</td>
<td>0032:0004</td>
</tr>
<tr>
<td>to the department's</td>
<td>E-EMAIL</td>
<td>is secure from unauthorized access,</td>
<td>0047:0004</td>
</tr>
<tr>
<td>the person or entity seeking access to</td>
<td>E-EMAIL</td>
<td>is secure from unauthorized access</td>
<td>0043:0005</td>
</tr>
<tr>
<td>create, receive, maintain, or transmit</td>
<td>E-EMAIL</td>
<td>is the one claimed.</td>
<td>0045:0005</td>
</tr>
<tr>
<td>to guard against unauthorized access to</td>
<td>E-EMAIL</td>
<td>on behalf of Sedgwick County</td>
<td>0038:0005</td>
</tr>
<tr>
<td>&quot; Develop</td>
<td>E-EMAIL</td>
<td>transmitted over any electronic</td>
<td>0046:0005</td>
</tr>
<tr>
<td>may not intentionally intercept,</td>
<td>E-WORKERS</td>
<td>better able to provide e-government</td>
<td>0053:0007</td>
</tr>
<tr>
<td>and intentional attacks, e.g.,</td>
<td>EAVESDROP</td>
<td>, record, read, alter or receive other</td>
<td>0004:0014</td>
</tr>
<tr>
<td>may be obtained by the responsible</td>
<td>EAVESDROPPING</td>
<td>snooping, fraud, theft, vandalism</td>
<td>0032:0051</td>
</tr>
<tr>
<td>Records Coordinators - Each</td>
<td>ELECTED</td>
<td>appointed official or division</td>
<td>0053:0025</td>
</tr>
<tr>
<td>with the department director/</td>
<td>ELECTED</td>
<td>County official, division director and</td>
<td>0057:0059</td>
</tr>
<tr>
<td>Director: The Department Director,</td>
<td>ELECTED</td>
<td>official or their designee</td>
<td>0083:0034</td>
</tr>
<tr>
<td></td>
<td>ELECTED</td>
<td>Official, or the Chief Judge</td>
<td>0065:0005</td>
</tr>
</tbody>
</table>
Director: The Department Director, Services in fulfilling its role, * Upon request of department heads, clear guidelines to all employees and of the officials in carrying out their Eighteenth Judicial District Court, board systems or attachments to electronic communications involving * * Fraudulent, harassing, violent, defamatory, harassing, appear in the newspaper without being (1) - loss of productivity; nuisance; County Employees are not permitted to County Employees are not permitted to Requirement 4; and the contents of such file shall be media or be sent by e-mail unless High risk data must be High risk data must be PRIVATE NETWORK (VPN): A secure, from the county solicitor and must be County shall adopt procedures for to another, Sedgwick County will use mail system (i.e., passwords, Palm Pilots or similar devices) without shall not install or use any type of message digest (e.g., MDS or SHA) and Data Transmission & Data Transmission & so that appropriate backup and have a minimum of 40-bit Shared Key 10. Install or use software, technical information, even when such safeguards are not to be installed. shall have power-on passwords or data access. The role of IS is to maintain an information base of all maintain an information database of all home computer using remote access. The home computer using remote access. The is a word found in a dictionary of the following four classes: (i) * (ii) approved the Department will process an PAF for the employee's stipend. Note: Integrity and lawful manner. Personal use of...
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>in the law, regulations, professional</td>
<td>ETHICS, and accreditation requirements</td>
<td>0048:0015</td>
</tr>
<tr>
<td>in nature or discriminate against</td>
<td>ETHNIC</td>
<td>0052:0008</td>
</tr>
<tr>
<td>or offensive to others based on</td>
<td>ETHNICITY</td>
<td>0052:0008</td>
</tr>
<tr>
<td>County provided laptops should have</td>
<td>ETRUST</td>
<td>0076:0022</td>
</tr>
<tr>
<td>or fire alarms, it may be necessary to</td>
<td>EVACUATE</td>
<td>0099:0098</td>
</tr>
<tr>
<td>(1) safety and</td>
<td>EVACUATION</td>
<td>0049:0048</td>
</tr>
<tr>
<td>o Hurricane</td>
<td>EVACUATION takes the last full backup of our</td>
<td>0003:0310</td>
</tr>
<tr>
<td>Email attachments that end in: .</td>
<td>EXE</td>
<td>0002:0711</td>
</tr>
<tr>
<td>chain letters, personal shopping,</td>
<td>EXECUTABLE</td>
<td>0002:0077</td>
</tr>
<tr>
<td>first acquire and test programs and</td>
<td>EXECUTABLES</td>
<td>0002:0077</td>
</tr>
<tr>
<td>Employee</td>
<td>EXITING</td>
<td>0088:0015</td>
</tr>
<tr>
<td>escalated level of support requiring</td>
<td>EXPERT</td>
<td>0092:0120</td>
</tr>
<tr>
<td>suppression equipment (sprinklers, fire</td>
<td>EXTINGUISHERS</td>
<td>0039:0035</td>
</tr>
<tr>
<td>Verify location of hand fire</td>
<td>EXTINGUISHERS and floor pullers</td>
<td>0049:0093</td>
</tr>
<tr>
<td>be made via phone, email, Intranet or</td>
<td>FACE-TO-FACE</td>
<td>0102:0009</td>
</tr>
<tr>
<td>each workforce member (e.g., by</td>
<td>FACE-TO-FACE inspection of a valid photo ID</td>
<td>0002:0009</td>
</tr>
<tr>
<td>*</td>
<td>devices</td>
<td>0002:0316</td>
</tr>
<tr>
<td>Copiers and</td>
<td>FAX</td>
<td>0009:0016</td>
</tr>
<tr>
<td>stored by computer (including e-mail),</td>
<td>FAX</td>
<td>0089:0005</td>
</tr>
<tr>
<td>and telephone voice response and &quot;</td>
<td>FAXBACK</td>
<td>0046:0005</td>
</tr>
<tr>
<td>&quot;e-mail) that replace written /</td>
<td>FAXED</td>
<td>0057:0134</td>
</tr>
<tr>
<td>&quot;Do Not Mail - return this PO to IT for</td>
<td>FAXING</td>
<td>0002:0341</td>
</tr>
<tr>
<td>Anti-Virus. This software scans our</td>
<td>FILE-SHARING</td>
<td>0076:0022</td>
</tr>
<tr>
<td>B.1. Management of</td>
<td>FILTER</td>
<td>0066:0042</td>
</tr>
<tr>
<td>o Use a screen</td>
<td>FILTER</td>
<td>0079:0006</td>
</tr>
<tr>
<td>2. A SMTP</td>
<td>FILTER</td>
<td>0002:0525</td>
</tr>
<tr>
<td>unwanted emails (&quot;spam&quot;) through email</td>
<td>FILTER</td>
<td>0002:0525</td>
</tr>
<tr>
<td>G.</td>
<td>FILTER</td>
<td>0002:0525</td>
</tr>
<tr>
<td>Do Webcontent</td>
<td>FILTER</td>
<td>0002:0525</td>
</tr>
<tr>
<td>4.a. Internet</td>
<td>FILTER</td>
<td>0066:0013</td>
</tr>
<tr>
<td>- Air</td>
<td>FILTER</td>
<td>0082:0014</td>
</tr>
<tr>
<td>C.2.a.</td>
<td>FILTER</td>
<td>0063:0011</td>
</tr>
<tr>
<td>correspondence, oath of loyalty,</td>
<td>FILTERs and Authentication: Two factor</td>
<td>0066:0047</td>
</tr>
<tr>
<td></td>
<td>FINGERPRINTS, medical examination reports</td>
<td>0008:0275</td>
</tr>
<tr>
<td>*</td>
<td>FIREFOX</td>
<td>0092:0240</td>
</tr>
<tr>
<td>1.3.4.</td>
<td>FIREFOX</td>
<td>0096:0062</td>
</tr>
<tr>
<td>connects to the Internet through a</td>
<td>FIREWALL</td>
<td>0003:0053</td>
</tr>
<tr>
<td>Employees must not circumvent the</td>
<td>FIREWALL</td>
<td>0003:0184</td>
</tr>
<tr>
<td>H.</td>
<td>FIREWALL</td>
<td>0090:0112</td>
</tr>
<tr>
<td>Requirement 1: Install and maintain a</td>
<td>FIREWALL</td>
<td>0066:0014</td>
</tr>
<tr>
<td>software updates to workstations, the</td>
<td>FIREWALL</td>
<td>0056:0007</td>
</tr>
<tr>
<td>as their default policy. Any unused</td>
<td>FIREWALL</td>
<td>0068:0166</td>
</tr>
<tr>
<td>* Any request to open</td>
<td>FIREWALL</td>
<td>0046:0105</td>
</tr>
<tr>
<td>any other Internet Web site, but the</td>
<td>FIREWALL</td>
<td>0002:0496</td>
</tr>
<tr>
<td>any other Internet Web site, but the</td>
<td>FIREWALL</td>
<td>0082:0001</td>
</tr>
<tr>
<td>1.</td>
<td>FIREWALL</td>
<td>0091:0026</td>
</tr>
<tr>
<td>protected from viruses with the help of</td>
<td>FIREWALL</td>
<td>0092:0108</td>
</tr>
<tr>
<td>devices, including but not limited to</td>
<td>FIREWALL</td>
<td>0079:0005</td>
</tr>
<tr>
<td>Service Requests: Configuration of all</td>
<td>FIREWALL, e-mail scanning software and</td>
<td>0003:0212</td>
</tr>
<tr>
<td>recent patches at least once a quarter,</td>
<td>FIREWALL, routers, and switches, will be</td>
<td>0063:0012</td>
</tr>
<tr>
<td>beyond the organization's exterior</td>
<td>FIREWALL, routers, switches, hubs and other</td>
<td>0068:0035</td>
</tr>
<tr>
<td>Sedgwick County shall maintain adequate</td>
<td>FIREWALLs, web servers, FTP servers, and other</td>
<td>0065:0037</td>
</tr>
<tr>
<td>boots, dirty athletic shoes, thongs,</td>
<td>FIREWALLs to protect its networks.</td>
<td>0046:0015</td>
</tr>
<tr>
<td>16.3.28 Family Medical Leave Act (</td>
<td>FLIP-FLOPS</td>
<td>0076:0020</td>
</tr>
<tr>
<td>vacation, sick, family medical leave (</td>
<td>FMLS</td>
<td>0092:0088</td>
</tr>
<tr>
<td>and subject to Freedom of Information (</td>
<td>FOI</td>
<td>0008:0106</td>
</tr>
<tr>
<td>Requests for information under the</td>
<td>FOIA</td>
<td>0081:0005</td>
</tr>
<tr>
<td>Carolina Freedom of Information Act (</td>
<td>FOIA</td>
<td>0006:0001</td>
</tr>
<tr>
<td>or not, check with your supervisor, or</td>
<td>FOIA</td>
<td>0003:0407</td>
</tr>
<tr>
<td>the Town's system are subject to the</td>
<td>FOIA</td>
<td>0065:0031</td>
</tr>
<tr>
<td>for electric/medicine/medical care/</td>
<td>FOOD</td>
<td>0089:0015</td>
</tr>
</tbody>
</table>
| 4/7/2008 Page 276 of 296
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>attacks, e.g., eavesdropping, snooping,</td>
<td>FORENSIC</td>
<td>auditing, security breach</td>
</tr>
<tr>
<td>or send or retrieve over the Internet.</td>
<td>FRAUD</td>
<td>theft, vandalism, sabotage, blackmail</td>
</tr>
<tr>
<td>Indecent, vulgar, harassing,</td>
<td>FRAUDULENT</td>
<td>harassing, embarrassing, indecent</td>
</tr>
<tr>
<td>Employee includes both</td>
<td>FULLTIME</td>
<td>and part-time City employees, and</td>
</tr>
<tr>
<td>to play games on the internet or to</td>
<td>GAMBLE</td>
<td></td>
</tr>
<tr>
<td>use for the purpose of shopping,</td>
<td>GAMBLING</td>
<td>gaming, nor browsing sites which could</td>
</tr>
<tr>
<td>offensive or threatening messages,</td>
<td>GAMBLING</td>
<td>illegal weapons, terrorist activities,</td>
</tr>
<tr>
<td>Game: betting,</td>
<td>GAMBLING</td>
<td>pornography, viruses, chain letters,</td>
</tr>
<tr>
<td>* Selected</td>
<td>GAMBLING</td>
<td>wagering</td>
</tr>
<tr>
<td>*</td>
<td>GAMBLING</td>
<td>wages</td>
</tr>
<tr>
<td>*</td>
<td>GAMBLING</td>
<td>(whether for fun or profit)</td>
</tr>
<tr>
<td>a.</td>
<td>GAMING</td>
<td>software will NOT be delivered with the</td>
</tr>
<tr>
<td>*</td>
<td>GAMES</td>
<td>0085:0014</td>
</tr>
<tr>
<td>*</td>
<td>GAMES</td>
<td>0092:0220</td>
</tr>
<tr>
<td>*</td>
<td>GAMES</td>
<td>0096:0051</td>
</tr>
<tr>
<td>tickers, news reels, movie downloads,</td>
<td>GAMES</td>
<td>screensavers used from the Internet</td>
</tr>
<tr>
<td>1.11.4 Playing computer</td>
<td>GAMES</td>
<td>Games will not be loaded, installed,</td>
</tr>
<tr>
<td>* Running or installing</td>
<td>GAMES</td>
<td>on Gaston County computers is</td>
</tr>
<tr>
<td>Internet connection to download -Entertainment software,</td>
<td>GAMES</td>
<td>or playing games on the Internet,</td>
</tr>
<tr>
<td>5. No</td>
<td>GAMES</td>
<td>other than those included with the</td>
</tr>
<tr>
<td>for the purpose of shopping, gambling,</td>
<td>GAMES</td>
<td>software is authorized software under</td>
</tr>
<tr>
<td>properly, these devices become open</td>
<td>GATEWAY</td>
<td>to the City's network and data. These</td>
</tr>
<tr>
<td>county-approved software and Internet</td>
<td>GATEWAYS</td>
<td></td>
</tr>
<tr>
<td>* Slacks, jeans,</td>
<td>GAUCHOS</td>
<td>and capris are acceptable in the</td>
</tr>
<tr>
<td>Formium, Adobe Acrobat Professional,</td>
<td>GENEXUS</td>
<td>.NET,</td>
</tr>
<tr>
<td>research, obtaining quotes, access to</td>
<td>GIS</td>
<td>and Tax information,</td>
</tr>
<tr>
<td>* Selected</td>
<td>GIS</td>
<td>applications,</td>
</tr>
<tr>
<td>* Selected</td>
<td>GIS</td>
<td>applications</td>
</tr>
<tr>
<td>applications (such as Geoplan, Vision,</td>
<td>GIS-ESRI</td>
<td>Orthophoto Database: Since this is</td>
</tr>
<tr>
<td>failures; human error; and acts of</td>
<td>GOD</td>
<td>0000:3030</td>
</tr>
<tr>
<td>and/or services (text messaging,</td>
<td>GPS</td>
<td>0000:3030</td>
</tr>
<tr>
<td>this policy should follow the Union</td>
<td>GRIEVANCE</td>
<td>Procedure in the Union Contract or the</td>
</tr>
<tr>
<td>The process is associated with</td>
<td>HACK</td>
<td>or introduce viruses into a system),</td>
</tr>
<tr>
<td>come increased activity on the part of</td>
<td>HACKERS</td>
<td>activity because it does not test the</td>
</tr>
<tr>
<td>that minimize opportunities for</td>
<td>HACKING</td>
<td>and vandals who exploit weaknesses in</td>
</tr>
<tr>
<td>intimate apparel, drugs and alcohol,</td>
<td>HACKING</td>
<td>and viruses from destroying computer.</td>
</tr>
<tr>
<td>executable 'ready to run files',</td>
<td>HACKING</td>
<td>or viruses to infiltrate the City.</td>
</tr>
<tr>
<td>or privileges; malicious code or virus;</td>
<td>HACKING</td>
<td>0001:0052</td>
</tr>
<tr>
<td>logos, pictures, cartoons, or slogans;</td>
<td>HALTER-TOPS</td>
<td>low-cut tops and tops with bare</td>
</tr>
<tr>
<td>may reasonably be considered offensive,</td>
<td>HARASSING</td>
<td>or to collect replies</td>
</tr>
<tr>
<td>anything that might be construed as</td>
<td>HARASSING</td>
<td>demeaning, or disruptive to any member,</td>
</tr>
<tr>
<td>electronic communication should not be</td>
<td>HARASSING</td>
<td>fraudulent, intimidating or otherwise</td>
</tr>
<tr>
<td>4/7/2008 Page 277 of 296</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
over the Internet. Fraudulent, right to privacy and to freedom from violence, waste of corporate assets, requests are made for the purpose of material that is in violation of sexual material or forms which violate our that would violate the County's Sexual F.7.a. Sexual Internet to access sites which promote include, but are not limited to, explicit, violence, criminal skills, * No

2.2. Access to Technology. Access to and use of the technology is always lawful, ethical, reflects HONESTY, and shows restraint in the consumption of personal health information covered by

the legal requirements relating to the

the legal requirements relating to the

policy is to ensure Sedgwick County's HIPAA-IMPACTED departments adopt and maintain

3.2. All employees, as part of new * If the department wishes to

HIRE, and biannual training, are to be made

HIRE, the person, at least two reference

HIRE / Transfer / Move Requests

New

Individuals

with technology access when is the value for which the vendor was informed of all personnel actions (new

Requests for new

Technology's policy relating to new

Employee

access from his/her supervisor. Upon

PROCEDURE AND POLICY FOR

form and submit the form to the

attacks (these are almost always a e-mail from unfamiliar senders, and virus warnings that are actually virus known phrases indicative of spam, use always is lawful, ethical, reflects use is always ethical, reflects that might be construed as harassing, be used to protect equipment from a

HARASSMENT or obscene messages are prohibited. All...

HARASSMENT , intimidation, and unwarranted...

HARASSMENT or hostile workplace policy in...

HARASSMENT policy or create an intimidating or...

HARASSMENT Policy, or that is of a sexual or...

HARASSMENT. Violating federal, state and local...

HATE groups, pornographic material or...

HATE speech or material that is prohibited...

HATE speech, personals and dating, glamour...

HATE Speech...

HATS or caps indoors...

HELPDESK...

HELPDESK (316-660-9811)...)

HELPDESK ) upon discovery...

HIPAA, Drug and Alcohol, and CYS are in this...

HIPAA, or standard of Charleston County...

HIPAA ) information...

HIPAA...

HIPAA or other personnel information...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HIPAA Security...

HARASSMENT... Violating federal, state and local

HARASSMENT that would violate the County's Sexual HARASSMENT or hostile workplace policy in...
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>which might constitute intimidating,</td>
<td>HOSTILE</td>
<td>or offensive material on the basis of</td>
<td>0069.0199</td>
</tr>
<tr>
<td>or offensive to another on the basis of</td>
<td>HOSTILE</td>
<td>work environment is prohibited</td>
<td>0002.0038</td>
</tr>
<tr>
<td>that would offend someone or create a</td>
<td>HOSTILE</td>
<td>work environment based on his/her race</td>
<td>0040.0023</td>
</tr>
<tr>
<td>in violation of sexual harassment or</td>
<td>HOSTILE</td>
<td>workplace policy in accordance with the</td>
<td>0005.0029</td>
</tr>
<tr>
<td>-- Self-Assessment Questionnaire</td>
<td>HTTPS</td>
<td>...............................................</td>
<td>0056.0027</td>
</tr>
<tr>
<td>- HUMIDITY controls</td>
<td>0039.0045</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drills include: fire, tornado, safety,</td>
<td>HURRICANE</td>
<td>and chemical spills</td>
<td>0008.0017</td>
</tr>
<tr>
<td>storms, floods, fires, tornadoes and</td>
<td>HURRICANES</td>
<td>evacuation takes the last full backup</td>
<td>0003.0310</td>
</tr>
<tr>
<td>(e.g., tornado, fire, earthquake, and</td>
<td>HURRICANES</td>
<td>...............................................</td>
<td>0008.0176</td>
</tr>
<tr>
<td>restrict the use of Instant Messaging</td>
<td>IM</td>
<td>) and Peer to Peer File Sharing (P2P) in...</td>
<td>0081.0002</td>
</tr>
<tr>
<td>requests to acquire film / digital</td>
<td>IMAGING</td>
<td>...............................................</td>
<td>0002.0295</td>
</tr>
<tr>
<td>Microsoft Exchange Server, IPSwitch</td>
<td>IMAGING</td>
<td>systems and services, consistent with</td>
<td>0057.0053</td>
</tr>
<tr>
<td>reports provided by Data Processing for</td>
<td>IM</td>
<td>...............................................</td>
<td>0284.0029</td>
</tr>
<tr>
<td>Fraudulent, harassing, embarrassing,</td>
<td>INDECENT</td>
<td>, profane, obscene, intimidating, or</td>
<td>0001.0023</td>
</tr>
<tr>
<td>Internet, to view and/or disseminate</td>
<td>INDECENT</td>
<td>or otherwise inappropriate information,</td>
<td>0089.0008</td>
</tr>
<tr>
<td>and other inappropriate content to</td>
<td>INFECTION</td>
<td>a computer on our network and then</td>
<td>0079.0012</td>
</tr>
<tr>
<td>policy outlines how various viruses can</td>
<td>INFECT</td>
<td>computers and networks. File downloads</td>
<td>0053.0021</td>
</tr>
<tr>
<td>outside the network and which may get</td>
<td>INFECTED</td>
<td>the City of Livonia's network, how the......</td>
<td>0076.0005</td>
</tr>
<tr>
<td>Technicians shall clean/repair any</td>
<td>INFECTED</td>
<td>So, the next time you use your</td>
<td>0001.0035</td>
</tr>
<tr>
<td>to a virus if they suspect one has</td>
<td>INFECTED</td>
<td>...............................................</td>
<td>0032.0022</td>
</tr>
<tr>
<td>a user PC, etc. One sign of a computer</td>
<td>INFECTED</td>
<td>the City of Livonia's network</td>
<td>0076.0005</td>
</tr>
<tr>
<td>the Internet can also be a source of</td>
<td>INFECTED</td>
<td>with Spyware is usually a slowdown in</td>
<td>0002.0095</td>
</tr>
<tr>
<td>shall take steps to prevent further</td>
<td>INFECION</td>
<td>. As with other types of transmissions,.........</td>
<td>0076.0014</td>
</tr>
<tr>
<td>protect that network from virus</td>
<td>INFECION</td>
<td>. Users shall cease using workstations</td>
<td>0040.0033</td>
</tr>
<tr>
<td>Explorer, Access, Publisher and</td>
<td>INFECION</td>
<td>...............................................</td>
<td>0076.0004</td>
</tr>
<tr>
<td>a. High (3) - death or serious</td>
<td>INFOPATH</td>
<td>...............................................</td>
<td>0085.0007</td>
</tr>
<tr>
<td>system whose failure may cause</td>
<td>INJURY</td>
<td>; sentinel patient care event; inactivity</td>
<td>0032.0077</td>
</tr>
<tr>
<td>of this policy will cause irreparable</td>
<td>INJURY</td>
<td>or death to human beings. Downtime is.....</td>
<td>0068.0119</td>
</tr>
<tr>
<td>defamatory, harassing, embarrassing,</td>
<td>INJURY</td>
<td>to the City and that violation during........</td>
<td>0099.0014</td>
</tr>
<tr>
<td>vulnerabilities to the confidentiality,</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0004.0023</td>
</tr>
<tr>
<td>protect the confidentiality,</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0032.0004</td>
</tr>
<tr>
<td>to protect the confidentiality,</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0008.0017</td>
</tr>
<tr>
<td>for ensuring the confidentiality,</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0046.0009</td>
</tr>
<tr>
<td>when necessary to preserve the</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0069.0034</td>
</tr>
<tr>
<td>manner fitting expected accessibility,</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0040.0017</td>
</tr>
<tr>
<td>of availability, confidentiality, and</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0083.0052</td>
</tr>
<tr>
<td>trust and reliance on your professional</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0063.0003</td>
</tr>
<tr>
<td>purposes. This also ensures the</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0059.0007</td>
</tr>
<tr>
<td>networks. Such software threatens the</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0065.0005</td>
</tr>
<tr>
<td>confidentiality, availability, and</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0090.0083</td>
</tr>
<tr>
<td>computing standards and protecting the</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0003.0049</td>
</tr>
<tr>
<td>6. Compromise the</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0091.0043</td>
</tr>
<tr>
<td>of ensuring the availability and</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0004.0038</td>
</tr>
<tr>
<td>any purpose related to maintaining the</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0049.0004</td>
</tr>
<tr>
<td>1.1.3.2 The</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0002.0020</td>
</tr>
<tr>
<td>must ensure that the security and</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0011.0032</td>
</tr>
<tr>
<td>freely disseminated to the public, the</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0064.0012</td>
</tr>
<tr>
<td>in order to protect the security/</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0068.0041</td>
</tr>
<tr>
<td>points in order to protect the security/</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0079.0002</td>
</tr>
<tr>
<td>(P2P) in order to protect the security/</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0080.0002</td>
</tr>
<tr>
<td>Policy for Use of Computers, E-Mail &amp;</td>
<td>INTEGRITY</td>
<td>...............................................</td>
<td>0081.0002</td>
</tr>
<tr>
<td>use of electronic mail (email),</td>
<td>INTERNET</td>
<td>...............................................</td>
<td>0060.0001</td>
</tr>
<tr>
<td>or external communications networks</td>
<td>INTERNET</td>
<td>...............................................</td>
<td>0001.0018</td>
</tr>
<tr>
<td>, include the City's computer network,</td>
<td>INTERNET</td>
<td>...............................................</td>
<td>0082.0001</td>
</tr>
<tr>
<td>communications network, including the</td>
<td>INTERNET</td>
<td>...............................................</td>
<td>0091.0004</td>
</tr>
<tr>
<td>networks, electronic mail (e-mail),</td>
<td>INTERNET</td>
<td>...............................................</td>
<td>0046.0005</td>
</tr>
<tr>
<td>0068.0007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEFT CONTEXT</td>
<td>KEYWORD</td>
<td>RIGHT CONTEXT</td>
<td>DOC:LINE</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>messages, (2) addresses accessed on the</td>
<td>INTERNET</td>
<td>, or (3) other data on County equipment</td>
<td>0054.0003</td>
</tr>
<tr>
<td>applications, electronic mail, and the</td>
<td>INTERNET</td>
<td>. Passwords are assigned for access to</td>
<td>0007.0007</td>
</tr>
<tr>
<td>variety of software is available on the</td>
<td>INTERNET</td>
<td>. Some of this software, called</td>
<td>0090.0084</td>
</tr>
<tr>
<td>mail have become very popular on the</td>
<td>INTERNET</td>
<td>. Unfortunately, these systems have</td>
<td>0079.0004</td>
</tr>
<tr>
<td>(as defined by the Village's</td>
<td>INTERNET</td>
<td>Acceptable Use Policy), the Village</td>
<td>0031.0015</td>
</tr>
<tr>
<td>voice mail, facsimile communication and</td>
<td>INTERNET</td>
<td>access, are Town property intended for</td>
<td>0089.0005</td>
</tr>
<tr>
<td>Information technology includes</td>
<td>INTERNET</td>
<td>access, electronic mail and voice</td>
<td>0052.0003</td>
</tr>
<tr>
<td>use. Information technology includes</td>
<td>INTERNET</td>
<td>access, electronic and voice message</td>
<td>0053.0004</td>
</tr>
<tr>
<td>be issued. All requests for e-mail and</td>
<td>INTERNET</td>
<td>access must be submitted on the</td>
<td>0077.0006</td>
</tr>
<tr>
<td>to file transfers, electronic mail,</td>
<td>INTERNET</td>
<td>access while using the County's network</td>
<td>0067.0017</td>
</tr>
<tr>
<td>accessing County computer systems.</td>
<td>INTERNET</td>
<td>Access Usage and Electronic Mail</td>
<td>0071.0001</td>
</tr>
<tr>
<td>to perform the job and will not include</td>
<td>INTERNET</td>
<td>access. Sedgwick County reserves the</td>
<td>0055.0002</td>
</tr>
<tr>
<td>use of Sedgwick County property, or</td>
<td>INTERNET</td>
<td>and downloading of computer files which</td>
<td>0069.0003</td>
</tr>
<tr>
<td>involving electronic-mail (e-mail),</td>
<td>INTERNET</td>
<td>and e-mail, is a privilege and not a</td>
<td>0083.0070</td>
</tr>
<tr>
<td>such as computer equipment, network,</td>
<td>INTERNET</td>
<td>password, and E-MAIL CODE OF CONDUCT</td>
<td>0061.0002</td>
</tr>
<tr>
<td>The Board of Commissioners adopted an</td>
<td>INTERNET</td>
<td>and Online Services Policy to support</td>
<td>0062.0007</td>
</tr>
<tr>
<td>that have become popular on the</td>
<td>INTERNET</td>
<td>can also be a source of infection. As</td>
<td>0076.0014</td>
</tr>
<tr>
<td>Internet-Downloading software via the</td>
<td>INTERNET</td>
<td>connectivity. Users are responsible for</td>
<td>0015.0008</td>
</tr>
<tr>
<td>network. VPN does not provide</td>
<td>INTERNET</td>
<td>does not automatically mean that the</td>
<td>0096.0033</td>
</tr>
<tr>
<td>downloaded without any charge from the</td>
<td>INTERNET</td>
<td>electronic mail may be &quot;in transit&quot;</td>
<td>0057.0001</td>
</tr>
<tr>
<td>Certain internal electronic mail and</td>
<td>INTERNET</td>
<td>and electronic mail into the Village's</td>
<td>0026.0007</td>
</tr>
<tr>
<td>software, or files downloaded from</td>
<td>INTERNET</td>
<td>network becomes</td>
<td>0068.0005</td>
</tr>
<tr>
<td>via any means, locally or via the</td>
<td>INTERNET</td>
<td>/Intranet/Extranet</td>
<td>0005.0036</td>
</tr>
<tr>
<td>software, or graphics on the</td>
<td>INTERNET</td>
<td>may be protected by federal copyright</td>
<td>0002.0009</td>
</tr>
<tr>
<td>County's wireless network to access the</td>
<td>INTERNET</td>
<td>only. Vendors will be provided the</td>
<td>0011.0014</td>
</tr>
<tr>
<td>copyrighted software from the</td>
<td>INTERNET</td>
<td>and bulletin boards without permission</td>
<td>0058.0027</td>
</tr>
<tr>
<td>Commercial computing networks</td>
<td>INTERNET</td>
<td>service, create security risks and</td>
<td>0051.0013</td>
</tr>
<tr>
<td>can degrade the county's network and</td>
<td>INTERNET</td>
<td>and prevent access to</td>
<td>0083.0065</td>
</tr>
<tr>
<td>refuse all offers by software and/or</td>
<td>INTERNET</td>
<td>sites to automatically login the next</td>
<td>0035.0066</td>
</tr>
<tr>
<td>4.a. Filtering/Blocking of</td>
<td>INTERNET</td>
<td>Sites: In order to promote productive</td>
<td>0063.0011</td>
</tr>
<tr>
<td>out or blocking of unacceptable</td>
<td>INTERNET</td>
<td>sites. ..................................................</td>
<td>0066.0013</td>
</tr>
<tr>
<td>as the &quot;home page&quot;. Cookies and</td>
<td>INTERNET</td>
<td>temporary files will be deleted at</td>
<td>0085.0018</td>
</tr>
<tr>
<td>* Software downloaded from the</td>
<td>INTERNET-DOWNLOADING</td>
<td>software via the Internet can also be a</td>
<td>0076.0014</td>
</tr>
<tr>
<td>of information from Gaston County's</td>
<td>INTERNET-RELATED</td>
<td>Systems or from the Internet</td>
<td>0002.0009</td>
</tr>
<tr>
<td>File Transfer Protocol, networking and</td>
<td>INTRANET</td>
<td>hardware and software (collectively</td>
<td>0002.0005</td>
</tr>
<tr>
<td>the City's computer network, Internet,</td>
<td>CRITICAL</td>
<td>and all personal computers, laptops</td>
<td>0002.0039</td>
</tr>
<tr>
<td>&quot; Internet,</td>
<td>CRITICAL</td>
<td>, email requirements</td>
<td>0002.0154</td>
</tr>
<tr>
<td>electronic mail (email), Internet, and</td>
<td>CRITICAL</td>
<td>access, and to define the</td>
<td>0091.0004</td>
</tr>
<tr>
<td>savers, log-in banners, newsletter/</td>
<td>CRITICAL</td>
<td>articles, posters, promotional items</td>
<td>0035.0022</td>
</tr>
<tr>
<td>any means, locally or via the Internet/</td>
<td>CRITICAL</td>
<td>/Extranet</td>
<td>0005.0036</td>
</tr>
<tr>
<td>Requests can be made via phone, email,</td>
<td>CRITICAL</td>
<td>or face-to-face. ......................................</td>
<td>0012.0009</td>
</tr>
<tr>
<td>to these procedures on the County</td>
<td>CRITICAL</td>
<td>site. ..................................................</td>
<td>0003.0046</td>
</tr>
<tr>
<td>reference checks can be found on the</td>
<td>CRITICAL</td>
<td>- The County network segment available</td>
<td>0083.0023</td>
</tr>
<tr>
<td>or others with authorization. An</td>
<td>CRITICAL</td>
<td>under Human Resources. This is done at</td>
<td>0010.0009</td>
</tr>
<tr>
<td>or others with authorization. An</td>
<td>CRITICAL</td>
<td>04/04/2008</td>
<td>0047:0016</td>
</tr>
<tr>
<td>be routed to the proper authorities to</td>
<td>INVESTIGATE</td>
<td>the matter and take reasonable steps to</td>
<td>0038.0029</td>
</tr>
<tr>
<td>not limited to, the Village's need to</td>
<td>INVESTIGATE</td>
<td>thoroughly all complaints. ......................</td>
<td>0061.0054</td>
</tr>
<tr>
<td>not limited to, the Village's need to</td>
<td>INVESTIGATE</td>
<td>a possible violation of policy or a</td>
<td>0016.0009</td>
</tr>
<tr>
<td>and the department. The Director will</td>
<td>INVESTIGATE</td>
<td>a possible violation of policy or a</td>
<td>0029.0014</td>
</tr>
<tr>
<td>over the Martin County network to</td>
<td>INVESTIGATE</td>
<td>any unusual or questionable patterns</td>
<td>0042.0013</td>
</tr>
<tr>
<td>possible. The Security Officer shall</td>
<td>INVESTIGATE</td>
<td>complaints of possible inappropriate</td>
<td>0005.0096</td>
</tr>
<tr>
<td>access to information and the need to</td>
<td>INVESTIGATE</td>
<td>the matter and take reasonable steps to</td>
<td>0038.0029</td>
</tr>
<tr>
<td>created when an incident report is</td>
<td>INVESTIGATED</td>
<td>thoroughly all complaints. ......................</td>
<td>0061.0054</td>
</tr>
<tr>
<td>a County-owned portable device will be</td>
<td>INVESTIGATED</td>
<td>The reports may include, but are not</td>
<td>0008.0214</td>
</tr>
<tr>
<td>of County-supplied equipment will be</td>
<td>INVESTIGATED</td>
<td>and, depending on circumstances, ..........</td>
<td>0065.0057</td>
</tr>
<tr>
<td>appropriate action to minimize harm,</td>
<td>INVESTIGATED</td>
<td>and may result in disciplinary action. ......</td>
<td>0067.0032</td>
</tr>
<tr>
<td>a process for receiving, documenting,</td>
<td>INVESTIGATING</td>
<td>breaches, and makes recommendations. ..</td>
<td>0047.0013</td>
</tr>
<tr>
<td>action to minimize harm, assists in</td>
<td>INVESTIGATING</td>
<td>, and responding to all complaints ..........</td>
<td>0047.0016</td>
</tr>
<tr>
<td>inappropriate use. In the course of</td>
<td>INVESTIGATING</td>
<td>breaches, and makes recommendations ..</td>
<td>0048.0010</td>
</tr>
<tr>
<td>* Assisting City officials in</td>
<td>INVESTIGATING</td>
<td>complaints, Martin County staff will......</td>
<td>0005.0096</td>
</tr>
<tr>
<td></td>
<td>INVESTIGATING</td>
<td>formally reported violations of this ..........</td>
<td>0091.0157</td>
</tr>
</tbody>
</table>
and management committee reports
information is requested as part of an
additional action (e.g., additional
suspected time frame for use in further
be provided to Network Security for
and the IT department will conduct an
of any security incident and conduct an
in the course of an ongoing
in these systems. This might include
are also expected to cooperate with any
INCIDENT/
forensic auditing, security breach
Departments in the course of legal
enforcement officials during official
to find lost messages, to comply with
according to the regulations of the
Slacks, JEANS
and video is permitted for approved
standardization, security and other
Resignation ___ Discharge ___
transfer of ownership, or by rental,
without the manufacturer’s software
completion or termination of contract/
one of our programmers, they are only
hardware and software that is owned,
should be budgeted and, purchased or
network, including the Internet,
CONTRACTS/
are only leased, in many cases these
must not access Internet sites with
???, Slander,
communication should not be harassing,
F.7.b. Violation of Copyright,
to programs and data by copyright and
which the County lacks the appropriate
with the manufacturer’s software
with the manufacturer’s software
staff in exchange for their Driver’s
is so authorized under a software
packages are generally sold under a
action is necessary to stay within our
follow the terms and conditions of the
in any manner inconsistent with the
owner. Failure to observe copyright or
agreed upon fees shall be paid for each
of County software will be under proper
or the end user does not have an active
data collection, data collection for
Allow
and it is licensed by the Town. A
Social Security Number, Driver
individuals. Software must be properly
an application that is completed when a
Systems Department and it is
but synchronization software must be
1. Butler County has purchased
products that are not appropriately
phones will not to be purchased by,
to prohibit users from duplicating any
resources are the property of the City.
2.4. Only legally

---

KWIC INDEX TO GMIS POLICIES

<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>and management committee reports</td>
<td>INVESTIGATING</td>
<td>various projects of the governing</td>
<td>0008:0195</td>
</tr>
<tr>
<td>information is requested as part of an</td>
<td>INVESTIGATING</td>
<td>, employee training and/or discipline</td>
<td>0033:0015</td>
</tr>
<tr>
<td>additional action (e.g., additional</td>
<td>INVESTIGATING</td>
<td>and verification.</td>
<td>0066:0052</td>
</tr>
<tr>
<td>suspected time frame for use in further</td>
<td>INVESTIGATING</td>
<td>as required by the nature of the</td>
<td>0068:0206</td>
</tr>
<tr>
<td>be provided to Network Security for</td>
<td>INVESTIGATING</td>
<td>concerning the cause of the incident</td>
<td>0036:0020</td>
</tr>
<tr>
<td>and the IT department will conduct an</td>
<td>INVESTIGATING</td>
<td>of criminal activity</td>
<td>0053:0023</td>
</tr>
<tr>
<td>of any security incident and conduct an</td>
<td>INVESTIGATING</td>
<td>of theft, unauthorized disclosure of</td>
<td>0002:0020</td>
</tr>
<tr>
<td>in the course of an ongoing</td>
<td>INVESTIGATING</td>
<td>regarding the use of your computer or</td>
<td>0003:0081</td>
</tr>
<tr>
<td>in these systems. This might include</td>
<td>INVESTIGATION</td>
<td>will be maintained as confidential to</td>
<td>0061:0054</td>
</tr>
<tr>
<td>are also expected to cooperate with any</td>
<td>INVESTIGATION</td>
<td>and related efforts.</td>
<td>0068:0202</td>
</tr>
<tr>
<td>any security incident and conduct an</td>
<td>INVESTIGATION</td>
<td>. While users cannot always control what</td>
<td>0089:0008</td>
</tr>
<tr>
<td>in the course of an ongoing</td>
<td>INVESTIGATION</td>
<td>of wrongful acts or to recover from</td>
<td>0002:0020</td>
</tr>
<tr>
<td>in these systems. This might include</td>
<td>INVESTIGATION</td>
<td>code</td>
<td>0011:0020</td>
</tr>
<tr>
<td>ffd the use of</td>
<td>INVESTIGATION</td>
<td>training and educational events</td>
<td>0026:0012</td>
</tr>
<tr>
<td>are expected to cooperate with any</td>
<td>INVESTIGATION</td>
<td>and valid technical and business</td>
<td>0083:0040</td>
</tr>
</tbody>
</table>
| Slacks, JEANS
and video is permitted for approved | JUSTIFIABLE | training and educational events | 0026:0012 |
| standardized, security and other | LEASE | or lending. The offering to | 0058:0029 |
| Resignation ___ Discharge ___ | LEASE | /agreement provided applicable audits | 0008:0155 |
| transfer of ownership, or by rental, | LEASE | , in many cases these leases are for a | 0058:0005 |
| which the County lacks the appropriate | LEASE | , or otherwise operated by Gaston | 0002:0005 |
| with the manufacturer’s software | LEASE | , using the normal operating department | 0009:0171 |
| with the manufacturer’s software | LEASE | , lines, dial-up lines, private networks | 0046:0005 |
| software that is owned, | LEASE | / AGREEMENTS: NON-CAPITAL | 0008:0152 |
| should be budgeted and, purchased or | LEASE | are for a very specific time period | 0058:0005 |
| network, including the Internet, | LEASE | , obscene, or sexually explicit | 0060:0090 |
| are only leased, in many cases these | LEASE | , deliberate misinformation | 0052:0022 |
| hardware and software that is owned, | LEASE | , deliberate misinformation | 0054:0010 |
| owner. Failure to observe copyright or | LEASE | , threatening, abusive, foul, or | 0060:0031 |
| agreed upon fees shall be paid for each | LICENSE | , and Registered Trademark | 0065:0037 |
| or the end user does not have an active | LICENSE | . (One license per ID.) | 0049:0046 |
| data collection, data collection for | LICENSE | . Furthermore, Bradford County | 0069:0047 |
| Allow
and it is licensed by the Town. A | LICENSE | agreement and may not be copied | 0028:0024 |
| Social Security Number, Driver
individuals. Software must be properly
an application that is completed when a
Systems Department and it is
but synchronization software must be
1. Butler County has purchased
products that are not appropriately
phones will not to be purchased by,
to prohibit users from duplicating any
resources are the property of the City.
2.4. Only legally

---

4/7/2008 Page 281 of 296
Authorized Software is legally software on City computers necessary...0092:0012
Bradford County employees will not copy software or permit it to be copied in...0069:0047
computers shall only contain legally software that contributes to the...0096:0007
that are owned by, leased, or computing resources will be properly to Gaston County. The scope of this...0002:0005
application identified, identify each application (i.e., authorized user) by job title...0032:0022
shall regularly update the list of for the various applications utilized...0041:0029
contractors or bidders for procurement, or license applicants, or entities that...0002:0043
Users must comply with all software * licences, and all other state and...0001:0022
date acquired, location, vendor, consists of copies of registrations, the organization lacks the appropriate...0002:0012
shall track and file all software shall and copyrights, as such disposal...0041:0017
for violation(s) of applicable software for violation(s) of applicable software intellectual property, such as software...0019:0011
comply with the copyrights and software LICENCES for all software that it purchases...0069:0047
Software LICENCES Policy...0027:0001
to the terms of all program/software responsible for checking copyright or...0058:0011
fully understand, and comply with the compliance with current and all future and Village personnel abide by the copyright notice appears on the work. LICENSING agreement that is included with each...0069:0009
agreements addressed in the use of...0058:0050
agreements entered into with software agreements may control redistribution...0002:0009
agreements, Resolution 9-25-97-131...0062:0007
Policy to enforce copyright and LICENSING agreements...0005:0111
1.11.3.5 Use does not violate software LICENSING : All off-site use of County software...0064:0015
4.b. Software LICENSING : All software installed on County...00065:0059
to ensure compliance with software LICENSING fees, fines, and increased Department...0096:0091
of unauthorized software, including LICENSOR . Unauthorized duplication of program /...0058:0011
16.3.74 Vehicle Usage LOG-IN . boots, dress shoes, dress sandals, and...0100:0027
retains the right to monitor, control, LOG...0092:0256
Non-employee personnel shall maintain a LOG , left with the computer, of all...0055:0019
sign-in on the Data Center access LOG , review, and other historymay...0049:0044
over the phone, the technician will LOG , and be paid for the time to the nearest...0019:0011
B.2.b. Change LOG : Changes to configuration will be...0066:0036
and Village personnel abide by the LICENSING or accreditation...0032:0077
policy to enforce copyright and LICENSING fees, fines, and increased Department...0002:0413
1.11.3.5 Use does not violate software LICENSING agreements, Resolution 9-25-97-131...0062:0007
4.b. Software LICENSING : All software installed on County...0064:0015
D. Software LICENSING : All software installed on County...0058:0009
to ensure compliance with software LICENSING fees, fines, and increased Department...0096:0091
of unauthorized software, including LICENSOR . Unauthorized duplication of program /...0058:0011
-log into the City of Montgomery IT system...0093:0048
each department will maintain a monthly LOG . immediately LOG . of such disposal...0041:0017
Logoff will be paid for the time to the nearest...0060:0023
should be responsible for maintaining a to "Thin Client". All users are to LOG , off the network when using this modem...0003:0297
the responsibility of the employee to LOG , off the Internet when not actively...0061:0007
the E-Mail program open and should LOG , off workstations when leaving them...0002:0029
workstations. Users should always LOG , on and allow the Department Head to...0054:0014
that the employee in question to system, each user shall be required to LOG , out of the system if they are not in...0016:0010
tasks are complete, the operator will LOG , out or lock the server immediately...0068:0084
compromises security. Be sure to LOG , out when you leave your workstation for...0060:0023
of generating audit logs. Each audit LOG shall include, at a minimum, user ID,...0043:0019
Information Technology personnel will LOG the problem and assign it to a...0017:0006
will be paid and the technician will LOG the time to the nearest hour. The...0012:0004
4. All access to Internet services is LOG-IN access to all servers and personal...0002:0237
during staff meetings, screen savers, LOG-IN banners, newsletter/intranet articles,...0035:0022
- PHI. Workforce members shall LOG-OFF workstations prior to the completion of...0040:0037
produce, that item does not need to be LOG-ON information. Passwords shall adhere to...0055:0005
LOGGED during staff meetings, screen savers, and tracked so SLC IT can manage...0102:0004
**KWIC INDEX TO GMIS POLICIES**

<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user’s Internet activities may be LOGGED by a surveillance system and reviewed......0089:0014</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>by providing a chronological series of LOGGED computer events that relate to an.........0043:0013</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All applications MUST come to be LOGGED in and approved by Human Resources.....0104:0005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>with a backup, the problem will be LOGGED in Track-It and the Information Systems ...0075:0018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>must have the computer turned on but LOGGED off on this designated night of the........0069:0043</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the functionality as if the user were LOGGED on locally to the network................0066:0020</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>off the system itself.). A user who is LOGGED on to a networked computer is.........0002:0029</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>may not leave their workstation LOGGED onto the network while away from their.....0055:0018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Desktops will remain LOGGED out or locked at all times unless a.............0068:0084</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sessions terminated (i.e., employees LOGGED out); review of latest security.........0032:0103</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When must be in place to prevent a user from LOGGING in to a certain computer then gaining........0090:0134</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>is not an intended recipient or LOGGING into a server or account that the...............0005:0031</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>when leaving your work area. Consider LOGGING off the computer or possibly turning.........0007:0060</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Desktops will remain LOGGED off the network when appropriate;..............0069:0098</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>around Gaston County equipment, and LOGGING off unattended workstations. Users.............0002:0029</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to lock the workstation rather than LOGGING off when leaving for very short time ..........0055:0018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of expressed consent to monitoring when LOGGING on to the network. These banners will ......0065:0019</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set at 10 minutes or less, or by LOGGING-OFF (control-alt-delete for Win2K users) )........0005:0166</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to change their passwords at initial LOGIN attempts. Identify multiple failed.........0033:0017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Scan successful and unsuccessful LOGGING in order to provide technical support.........0068:0015</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>that appropriate support personnel can LOGGING information. Should you get an e-mail.....0069:0103</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>you an e-mail asking you to confirm LOGIN name which allows access to one of the...0016:0007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Authorized users will be provided a LOGIN the next time that they access those........0035:0066</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and/or Internet sites to automatically LOGIN where appropriate.......................0085:0102</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shall include, at a minimum, user ID,LOGIN with an invalid password....................0077:0010</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* CITRIX LOGIN LOGINS and passwords. Each end-user must...............................0090:0166</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>there are three repetitive attempts to LOGIN - Scan successful and unsuccessful........0033:0017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to maintain a secured list of user LOGINs.......................................................0032:0272</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic LOGOFF.........................................................................................0042:0041</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic LOGOFF.........................................................................................0085:0018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>temporary files will be deleted at LOGOFF from network. Where logging off is not.....0069:0099</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>longer than fifteen minutes, user must LOGOFF mechanisms (e.g. Ctrl-Alt-Delete and....0040:0037</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>must lock or activate the automatic LOGOFF /sign-off networks when appropriate;........0051:0007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>are in place for their employees to LOGON banner reminding users of their..............0006:0172</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>County, the device will display a LOGON Banners: Logon banners will be used to........0065:0019</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOGON to the network. After changing this............0069:0035</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. must be changed the first time they LOGIN , and access reports.......................0033:0005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>file access, security incidents, audit LOGS . Each audit log shall include, at a ........0043:0019</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e-PHI for purposes of generating audit LOGS and records management software.........0057:0080</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>including boxes, labeling, storage LOGS are complete.................................0050:0033</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6) Verify member will review all server backup LOGS daily and will record the status of...0068:0181</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of training, incident, and media phone for compliance.....................................0032:0103</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the process of reviewing network email LOGS for the purpose of ensuring system.........0002:0254</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Items* in Outlook when the user LOGS off of the application. Trash cans............0085:0017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>King. While at work the next day, she LOGS onto Amazon.com and purchases the.....0003:0110</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>will print each department’s log. The LOGS will be maintained in individual.............0008:0044</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>integrity, confidentiality, LOGS and recoverability needs and in......................0083:0052</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cartoons, or slogans; halter-tops; LOGS tops and tops with bare shoulder are...........0005:0013</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>include Message Authentication Codes * MAC”), which are built upon message digest.....0046:0017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>actually hide themselves, often as LOGS , within other files, such as................0076:0007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* NEVER open any files or MACROS attached to an e-mail from an unknown,.......0003:0215</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sources, nor open any files or MACROS attached to an e-mail from an unknown..........0040:0021</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Access Usage and Electronic MAIL..........................................................0071:0001</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>805 ELECTRONIC MAIL..........................................................0090:0090</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>business applications, electronic MAIL and the internet. Passwords are.................0007:0007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Town’s system, including e-mail, voice MAIL , facsimile communication and Internet.....0089:0005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic network resources, such as MAIL , ftp, etc. which are located on all............0066:0019</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>limited to file transfers, electronic MAIL , Internet access, telnet, browsing..........0065:0014</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>presence in the office, electronic MAIL , the Banner hotline (x3839), and the.........0014:0002</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### KWIC INDEX TO GMIS POLICIES

<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>network accounts providing electronic</td>
<td>MAIL</td>
<td>, voice-mail, World Wide Web browsing...</td>
<td>0002:0005</td>
</tr>
<tr>
<td>network accounts providing electronic</td>
<td>MAIL</td>
<td>, web browsing, and FTP, all of which</td>
<td>0005:0004</td>
</tr>
<tr>
<td>Electronic</td>
<td></td>
<td>(&quot;E-Mail&quot;) System</td>
<td>0061:0019</td>
</tr>
<tr>
<td>and external networks, electronic</td>
<td>MAIL</td>
<td>(e-mail), Internet, modems, and...</td>
<td>0068:0007</td>
</tr>
<tr>
<td>and external networks, electronic</td>
<td>MAIL</td>
<td>(e-mail), Internet, modems, and...</td>
<td>0069:0009</td>
</tr>
<tr>
<td>Electronic</td>
<td></td>
<td>(E-mail) access provided to Martin</td>
<td>0004:0005</td>
</tr>
<tr>
<td>Electronic</td>
<td></td>
<td>(E-mail) Use</td>
<td>0060:0037</td>
</tr>
<tr>
<td>to and acceptable use of electronic</td>
<td>MAIL</td>
<td>(email), Internet, and Intranet access,</td>
<td>0091:0004</td>
</tr>
<tr>
<td>Certain internal electronic</td>
<td>MAIL</td>
<td>and Internet electronic mail may be</td>
<td>0057:0014</td>
</tr>
<tr>
<td>of another person's electronic or voice</td>
<td>MAIL</td>
<td>and other forms of electronic snooping...</td>
<td>0053:0024</td>
</tr>
<tr>
<td>includes Internet access, electronic</td>
<td>MAIL</td>
<td>and voice message systems, facsimile...</td>
<td>0052:0003</td>
</tr>
<tr>
<td>network, Internet access, electronic</td>
<td>MAIL</td>
<td>and voice message systems, facsimile</td>
<td>0055:0047</td>
</tr>
<tr>
<td>local ordinances. Electronic and voice</td>
<td>MAIL</td>
<td>capabilities provided to employees are</td>
<td>0051:0008</td>
</tr>
<tr>
<td>Web Based</td>
<td>MAIL</td>
<td>: REGISTERED AND CERTIFIED...</td>
<td>0008:0226</td>
</tr>
<tr>
<td>Voice</td>
<td>MAIL</td>
<td>Systems</td>
<td>0079:0001</td>
</tr>
<tr>
<td>Electronic</td>
<td>MAIL</td>
<td>Usage Policy</td>
<td>0029:0002</td>
</tr>
<tr>
<td>contents of any employee's electronic</td>
<td>MAILBOX</td>
<td>. Such access may occur, but is not</td>
<td>0016:0009</td>
</tr>
<tr>
<td>3. Print to a printer/copier</td>
<td>MAILBOX</td>
<td>and release the print job when standing</td>
<td>0068:0057</td>
</tr>
<tr>
<td>3. Print to a printer/copier</td>
<td>MAILBOX</td>
<td>and release the print job when standing</td>
<td>0069:0121</td>
</tr>
<tr>
<td>an e-mail message from a User's own</td>
<td>MAILBOX</td>
<td>does not mean all copies of the message</td>
<td>0003:0167</td>
</tr>
<tr>
<td>or unauthorized use of a password/</td>
<td>MAILBOX</td>
<td>is prohibited.</td>
<td>0002:0017</td>
</tr>
<tr>
<td>they have deleted a message from their</td>
<td>MAILBOX</td>
<td>it may not yet have been completely</td>
<td>0004:0004</td>
</tr>
<tr>
<td>assign an email address and/or voice</td>
<td>MAILBOX</td>
<td>to me based upon my representation that.</td>
<td>0089:0020</td>
</tr>
<tr>
<td>mail communications for authorized</td>
<td>MAILBOX</td>
<td>users</td>
<td>0029:0004</td>
</tr>
<tr>
<td>for review or pick up. Copies may be</td>
<td>MAILING</td>
<td>upon receipt of copying charge</td>
<td>0008:0045</td>
</tr>
<tr>
<td>12.4.8 Mass</td>
<td>MAILING</td>
<td>................................................</td>
<td>0091:0027</td>
</tr>
<tr>
<td>16.3.9 Mass</td>
<td>MAILING</td>
<td>................................................</td>
<td>0092:0012</td>
</tr>
<tr>
<td>non-business-related list-servers and</td>
<td>MAILING</td>
<td>lists, spending excessive amounts of...</td>
<td>0069:0213</td>
</tr>
<tr>
<td>&quot;MAIL: UNDELIVERABLE FIRST CLASS,&quot;</td>
<td>MAILING</td>
<td>MAILINGS? about viruses, or other warnings about</td>
<td>0003:0134</td>
</tr>
<tr>
<td>* Mass</td>
<td>MAILINGS</td>
<td>of official information throughout the...</td>
<td>0091:0056</td>
</tr>
<tr>
<td>by, among other things, sending mass</td>
<td>MAILINGS</td>
<td>or chain letters, spending excessive</td>
<td>0069:0179</td>
</tr>
<tr>
<td>mailings</td>
<td>MAILINGS</td>
<td>that require proof of mailing</td>
<td>0008:0233</td>
</tr>
<tr>
<td>returned. It does NOT include certified</td>
<td>MAILINGS</td>
<td>older than 60 days should be deleted...</td>
<td>0002:0111</td>
</tr>
<tr>
<td>* Voice</td>
<td>MAILS</td>
<td>death, divorce and birth certificates; ...</td>
<td>0008:0454</td>
</tr>
<tr>
<td>veteran administration (VA) benefits;</td>
<td>MARRIAGE</td>
<td>as appropriate to quantify the</td>
<td>0054:0052</td>
</tr>
<tr>
<td>7.8. Other</td>
<td>METRICS</td>
<td>&quot;environment with a few legacy...</td>
<td>0005:0005</td>
</tr>
<tr>
<td>Department. We are presently a...</td>
<td>MICROSOFT</td>
<td>Internet Explorer</td>
<td>0092:0196</td>
</tr>
<tr>
<td>*</td>
<td>MICROSOFT</td>
<td>Internet Explorer</td>
<td>0096:0039</td>
</tr>
<tr>
<td></td>
<td>MICROSOFT</td>
<td>Office XP Standard and Professional</td>
<td>0090:0069</td>
</tr>
<tr>
<td></td>
<td>MICROSOFT</td>
<td>Outlook Calendar with a reminder that...</td>
<td>0095:0026</td>
</tr>
<tr>
<td></td>
<td>MICROSOFT</td>
<td>will never send you an e-mail asking...</td>
<td>0069:0103</td>
</tr>
<tr>
<td></td>
<td>MICROSOFT</td>
<td>Windows ...</td>
<td>0078:0006</td>
</tr>
<tr>
<td></td>
<td>MICROSOFT</td>
<td>Windows platform (W2K or better)</td>
<td>0002:0278</td>
</tr>
<tr>
<td>dresses and skirts should be below</td>
<td>MID-THIGH</td>
<td>length</td>
<td>0100:0022</td>
</tr>
<tr>
<td></td>
<td>MIDRIFF</td>
<td>barring tops; shirts with other county's...</td>
<td>0100:0013</td>
</tr>
<tr>
<td>mid-thigh are inappropriate for work.</td>
<td>MINI-SKIRTS</td>
<td>, shorts, sun dresses, beach dresses...</td>
<td>0100:0023</td>
</tr>
<tr>
<td>diversion, destruction, loss,</td>
<td>MISUSE</td>
<td>, or theft of this information.</td>
<td>0100:0028</td>
</tr>
<tr>
<td>are functioning properly, and without</td>
<td>MISUSE</td>
<td>. Such sampling will also allow the City...</td>
<td>0101:0027</td>
</tr>
<tr>
<td>in their charge from physical damage or</td>
<td>MISUSE</td>
<td>; take appropriate steps to protect...</td>
<td>0051:0007</td>
</tr>
<tr>
<td>3.6) Employees who</td>
<td>MISUSE</td>
<td>E-mail privileges shall be subject to...</td>
<td>0004:0016</td>
</tr>
<tr>
<td>Examples of voice mail</td>
<td>MISUSE</td>
<td>include the following and are...</td>
<td>0002:0103</td>
</tr>
<tr>
<td>F.2.</td>
<td>MISUSE</td>
<td>of Assets: Monopolizing computer...</td>
<td>0065:0030</td>
</tr>
<tr>
<td>3.2 The</td>
<td>MISUSE</td>
<td>of computing resources shall subject...</td>
<td>0005:0133</td>
</tr>
<tr>
<td>user who determines that there may be</td>
<td>MISUSE</td>
<td>of software within the organization...</td>
<td>0058:0070</td>
</tr>
<tr>
<td>addition, violations of this policy or</td>
<td>MISUSE</td>
<td>of the computer system may be referred...</td>
<td>0007:0035</td>
</tr>
<tr>
<td>or employee from negative impact of the</td>
<td>MISUSE</td>
<td>of the Internet, other important...</td>
<td>0060:0072</td>
</tr>
<tr>
<td>for activities that are inappropriate.</td>
<td>MISUSE</td>
<td>or inappropriate personal use of City</td>
<td>0091:0090</td>
</tr>
<tr>
<td>without authorization, or otherwise</td>
<td>MISUSED</td>
<td>. Violations of this sort may be illegal...</td>
<td>0091:0131</td>
</tr>
<tr>
<td>maintain. Unfortunately, they can be</td>
<td>MISUSED</td>
<td>in a variety of ways, some of which are...</td>
<td>0101:0023</td>
</tr>
<tr>
<td>progressive discipline of the employee</td>
<td>MISUSING</td>
<td>the cellular telephone, the requirement...</td>
<td>0002:0128</td>
</tr>
<tr>
<td>LEFT CONTEXT</td>
<td>KEYWORD</td>
<td>RIGHT CONTEXT</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>execution of a Memorandum of Agreement (</td>
<td>MOA</td>
<td>or other contractual arrangement</td>
<td>0063:0008</td>
</tr>
<tr>
<td>own Internet service via dial-up, cable</td>
<td>MODEN</td>
<td>directly to the County's network is not</td>
<td>0066:0048</td>
</tr>
<tr>
<td>C.2.b. Modems: Connection via</td>
<td>MODEN</td>
<td>Use</td>
<td>0069:0153</td>
</tr>
<tr>
<td>7.6</td>
<td>MODEN</td>
<td>Use Procedures</td>
<td>0003:0294</td>
</tr>
<tr>
<td>electronic mail (e-mail), Internet,</td>
<td>MODEMS</td>
<td>, and facsimile systems. These tools</td>
<td>0068:0007</td>
</tr>
<tr>
<td>Internet access (such as via dial-out</td>
<td>MODEMS</td>
<td>, and facsimile systems. These tools</td>
<td>0069:0009</td>
</tr>
<tr>
<td>C.2.b.</td>
<td>MODEMS</td>
<td>from sites connected to the County</td>
<td>0090:0112</td>
</tr>
<tr>
<td>* Usage of Communicator, Internet Explorer, and</td>
<td>MOSAIC</td>
<td>are examples of browsers. This type of</td>
<td>0003:0404</td>
</tr>
<tr>
<td>other copyrighted sources, copyrighted</td>
<td>MUSIC</td>
<td>),. Issues of support, access,</td>
<td>0066:0045</td>
</tr>
<tr>
<td>audio or video, downloading of</td>
<td>MUSIC</td>
<td>, and the installation of any</td>
<td>0005:0025</td>
</tr>
<tr>
<td>use of software may include streaming</td>
<td>MUSIC</td>
<td>stock tickers, news reels, movie</td>
<td>0060:0082</td>
</tr>
<tr>
<td>of copyrighted software, video, or</td>
<td>MUSIC</td>
<td>, storing such copies on City computers,</td>
<td>0091:0100</td>
</tr>
<tr>
<td>is not limited to, illegal copies of</td>
<td>MUSIC</td>
<td>, videos, or software.</td>
<td>0062:0011</td>
</tr>
<tr>
<td>* chatting with their friends and sharing to, memory sticks, flash drives,</td>
<td>MUSIC</td>
<td>downloads</td>
<td>0092:0221</td>
</tr>
<tr>
<td>* such as literary works, databases,</td>
<td>MUSIC</td>
<td>flies. Both of the technologies are</td>
<td>0081:0004</td>
</tr>
<tr>
<td>*</td>
<td>MUSIC</td>
<td>/ video players, and so on. Personal</td>
<td>0065:0027</td>
</tr>
<tr>
<td>*</td>
<td>MUSIC</td>
<td>dramatic, or artistic nature, that has</td>
<td>0065:0099</td>
</tr>
<tr>
<td>*</td>
<td>MUSIC</td>
<td>works, sound recordings, photograph and</td>
<td>0058:0021</td>
</tr>
<tr>
<td>* NAPSTER</td>
<td>NAPSTER</td>
<td>) MUST be approved by IT. The purpose.</td>
<td>0002:0571</td>
</tr>
<tr>
<td>*</td>
<td>NETSCAPE</td>
<td>.</td>
<td>0092:0243</td>
</tr>
<tr>
<td>*</td>
<td>NETSCAPE</td>
<td>Communication, Internet Explorer, and</td>
<td>0096:0085</td>
</tr>
<tr>
<td>*</td>
<td>NEWGROUP</td>
<td>spam)</td>
<td>0003:0404</td>
</tr>
<tr>
<td>messages to Usenet newsgroups (</td>
<td>NEWGROUP</td>
<td>must contain a disclaimer stating that</td>
<td>0005:0045</td>
</tr>
<tr>
<td>from a Martin County email address to</td>
<td>Sedgwick County</td>
<td>Information Technology Usage</td>
<td>0055:0001</td>
</tr>
<tr>
<td>computer systems available to</td>
<td>NON-EMPLOYEE</td>
<td>are provided to support work</td>
<td>0005:0015</td>
</tr>
<tr>
<td>that may reasonably be considered</td>
<td>NON-EMPLOYEES</td>
<td>, abusive, threatening, or other</td>
<td>0071:0014</td>
</tr>
<tr>
<td>obscene, sexually oriented, racially</td>
<td>OFFENSIVE</td>
<td>, harassing, demeaning, or disruptive to</td>
<td>0040:0023</td>
</tr>
<tr>
<td>obscene, sexually explicit, illegal,</td>
<td>OFFENSIVE</td>
<td>, threatening and/or</td>
<td>0065:0029</td>
</tr>
<tr>
<td>of others. No abusive, profane or</td>
<td>OFFENSIVE</td>
<td>, threatening or other inappropriate</td>
<td>0060:0117</td>
</tr>
<tr>
<td>abusive, harassing, threatening, or</td>
<td>OFFENSIVE</td>
<td>language is transmitted through the</td>
<td>0061:0009</td>
</tr>
<tr>
<td>system is not to be used to create any</td>
<td>OFFENSIVE</td>
<td>messages, including offensive comments.</td>
<td>0003:0123</td>
</tr>
<tr>
<td>defamatory, derogatory or otherwise</td>
<td>OFFENSIVE</td>
<td>or disruptive messages. Among those</td>
<td>0060:0051</td>
</tr>
<tr>
<td>policies related to defamatory,</td>
<td>OFFENSIVE</td>
<td>or illegal information. Among that</td>
<td>0004:0034</td>
</tr>
<tr>
<td>or messages that may be hostile or</td>
<td>OFFENSIVE</td>
<td>or threatening messages, gambling,</td>
<td>0002:0007</td>
</tr>
<tr>
<td>newspaper without being embarrassing or</td>
<td>OFFENSIVE</td>
<td>to another on the basis of sex, race,</td>
<td>0089:0008</td>
</tr>
<tr>
<td>that are illegal, inappropriate, or</td>
<td>OFFENSIVE</td>
<td>to anyone. Avoid whatever could be</td>
<td>0005:0014</td>
</tr>
<tr>
<td>be construed as harassing, hostile, or</td>
<td>OFFENSIVE</td>
<td>to fellow employees or the public. Such</td>
<td>0091:0091</td>
</tr>
<tr>
<td>county's logos; shirts with potentially</td>
<td>OFFENSIVE</td>
<td>to others based on ethnicity, race,</td>
<td>0052:0008</td>
</tr>
<tr>
<td>or any other comment or material that</td>
<td>OFFENSIVELY</td>
<td>addresses someone's age, sexual</td>
<td>0004:0034</td>
</tr>
<tr>
<td>comments, or any other comment that</td>
<td>OFFENSIVELY</td>
<td>addresses someone's age, sexual</td>
<td>0060:0051</td>
</tr>
<tr>
<td>* Required to be</td>
<td>ON-CALL</td>
<td>(24/7)</td>
<td>0011:0010</td>
</tr>
<tr>
<td>The department has</td>
<td>ON-CALL</td>
<td>HelpDesk available 24/7</td>
<td>0043:0009</td>
</tr>
<tr>
<td>IT</td>
<td>ON-CALL</td>
<td>Protocol</td>
<td>0019:0001</td>
</tr>
<tr>
<td>16.3.7 Back-up</td>
<td>ON-CALL</td>
<td>Technician</td>
<td>0092:0020</td>
</tr>
<tr>
<td>Customer Support Coordinators, Primary</td>
<td>ON-CALL</td>
<td>Technician, and</td>
<td>0094:0019</td>
</tr>
<tr>
<td>Policy to provide access to an Primary</td>
<td>ON-CALL</td>
<td>Technician outside of regular business</td>
<td>0097:0007</td>
</tr>
<tr>
<td>*</td>
<td>OPENOFFICE</td>
<td>computers and networks</td>
<td>0066:0066</td>
</tr>
<tr>
<td>*</td>
<td>ORGANIZATION'S</td>
<td>exterior firewalls.</td>
<td>0076:0020</td>
</tr>
<tr>
<td>the integrity and security of the</td>
<td>ORGANIZATION'S</td>
<td>information system network is</td>
<td>0032:0018</td>
</tr>
<tr>
<td>network traffic are allowed beyond the</td>
<td>ORGANIZATION'S</td>
<td>network... A VPN works by using the</td>
<td>0092:0263</td>
</tr>
<tr>
<td>network diagram illustrating how</td>
<td>OUTLOOK</td>
<td></td>
<td>0085:0006</td>
</tr>
<tr>
<td>LEFT CONTEXT</td>
<td>KEYWORD</td>
<td>RIGHT CONTEXT</td>
<td>DOC:LINE</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>* Microsoft Office (Word, Excel,</td>
<td>OUTLOOK</td>
<td>Calendar with a reminder that will</td>
<td>0005:0121</td>
</tr>
<tr>
<td>* Microsoft Office (Word, Excel,</td>
<td>OUTLOOK</td>
<td>or any e-mail application, browsers)</td>
<td>0006:0040</td>
</tr>
<tr>
<td>the customer in his/her Microsoft</td>
<td>OUTLOOK</td>
<td>information technology vendor staff</td>
<td>0003:0406</td>
</tr>
<tr>
<td>feature of applications (e.g.,</td>
<td>OUTSOURCED</td>
<td>efforts. Outsourcing should be used:</td>
<td>0002:0351</td>
</tr>
<tr>
<td>of Charleston County and current</td>
<td>OUTSOURCING</td>
<td>pay</td>
<td>0002:0367</td>
</tr>
<tr>
<td>of long-term goals and objectives for</td>
<td>OVERTIME</td>
<td>It will apply</td>
<td>0014:0033</td>
</tr>
<tr>
<td>to take time off instead of receiving</td>
<td>OVERTIME</td>
<td>worked as a result of these procedures</td>
<td>0012:0006</td>
</tr>
<tr>
<td>off hours to resolve a problem, normal</td>
<td>OVERTIME</td>
<td>worked as a result of these procedures</td>
<td>0019:0013</td>
</tr>
<tr>
<td>Any</td>
<td>OWA</td>
<td>using ssl</td>
<td>0002:0330</td>
</tr>
<tr>
<td>hotline (x3839), and the use of a</td>
<td>PAGER</td>
<td>.</td>
<td>0014:0002</td>
</tr>
<tr>
<td>1. Call the IT On-Call</td>
<td>PAGER</td>
<td>to access without notice: data,</td>
<td>0019:0004</td>
</tr>
<tr>
<td>to access without notice: data,</td>
<td>PAGER</td>
<td>and Emergency Services; cell phone and</td>
<td>0002:0020</td>
</tr>
<tr>
<td>for call will be required to carry</td>
<td>PAGERS</td>
<td>and be available for calls if needed</td>
<td>0013:0007</td>
</tr>
<tr>
<td>of harassment via email, telephone or</td>
<td>PAGING</td>
<td>, whether through language, frequency</td>
<td>0005:0040</td>
</tr>
<tr>
<td>reply to the first attempt, please try</td>
<td>PAGING</td>
<td>again allowing for a second 15 minute</td>
<td>0019:0004</td>
</tr>
<tr>
<td>immediately, consider phoning or</td>
<td>PAGING</td>
<td>them</td>
<td>0009:0220</td>
</tr>
<tr>
<td>Slacks, Jeans,</td>
<td>PART-TIME</td>
<td>and temporary employees), officials</td>
<td>0003:0072</td>
</tr>
<tr>
<td>on County employees, (full-time,</td>
<td>PART-TIME</td>
<td>City employees, and employees working</td>
<td>0002:0077</td>
</tr>
<tr>
<td>employees includes both full-time and</td>
<td>PART-TIME</td>
<td>employees, volunteers, and other</td>
<td>0004:0017</td>
</tr>
<tr>
<td>3.7) Employees, contractors,</td>
<td>PART-TIME</td>
<td>employees, volunteers, and other</td>
<td>0005:0025</td>
</tr>
<tr>
<td>applies to all employees, contractors</td>
<td>PART-TIME</td>
<td>employees, volunteers, and other</td>
<td>0007:0029</td>
</tr>
<tr>
<td>attempt to obtain or distribute door</td>
<td>PASSCODES</td>
<td>/passkeys to secured rooms at any</td>
<td>0055:0041</td>
</tr>
<tr>
<td>to obtain or distribute door passcodes/</td>
<td>PASSKEYS</td>
<td>to secured rooms at any Sedgwick</td>
<td>0055:0041</td>
</tr>
<tr>
<td>of your spouse or child is not a secure</td>
<td>PASSWORD</td>
<td>. Every effort must be made to keep</td>
<td>0072:0004</td>
</tr>
<tr>
<td>including assignment of username and</td>
<td>PASSWORD</td>
<td>accounts are not permitted</td>
<td>0010:0015</td>
</tr>
<tr>
<td>The necessary user identification and</td>
<td>PASSWORD</td>
<td>The confidentiality of this password</td>
<td>0016:0007</td>
</tr>
<tr>
<td>with security code, access code or</td>
<td>PASSWORD</td>
<td>. Users will not share their passwords</td>
<td>0008:0026</td>
</tr>
<tr>
<td>be controlled by a secure username and</td>
<td>PASSWORD</td>
<td>. Users will share their passwords</td>
<td>0009:0027</td>
</tr>
<tr>
<td>then provide a personalized Network</td>
<td>PASSWORD</td>
<td>. Users will not share their passwords</td>
<td>0008:0016</td>
</tr>
<tr>
<td>identified with a unique username and</td>
<td>PASSWORD</td>
<td>(and/or other authentication mechanism)</td>
<td>0042:0045</td>
</tr>
<tr>
<td>identified with a unique username and</td>
<td>PASSWORD</td>
<td>on any system that resides at any</td>
<td>0002:0005</td>
</tr>
<tr>
<td>inactivity, the user must re-enter the</td>
<td>PASSWORD</td>
<td>- a secure combination of characters</td>
<td>0051:0023</td>
</tr>
<tr>
<td>of access that supports or requires a</td>
<td>PASSWORD</td>
<td>assignments. All systems containing</td>
<td>0030:0008</td>
</tr>
<tr>
<td>with system security, menus and</td>
<td>PASSWORD</td>
<td>assignments. All systems containing</td>
<td>0070:0009</td>
</tr>
<tr>
<td>with system security, menus and</td>
<td>PASSWORD</td>
<td>by the human resources department</td>
<td>0089:0012</td>
</tr>
<tr>
<td>sign-on identification and an &quot;initial&quot;</td>
<td>PASSWORD</td>
<td>can be used again by the same user</td>
<td>0066:0004</td>
</tr>
<tr>
<td>that must elapse before a particular</td>
<td>PASSWORD</td>
<td>/code. The confidentiality of this</td>
<td>0029:0018</td>
</tr>
<tr>
<td>box through the use of a voice mail box</td>
<td>PASSWORD</td>
<td>from unauthorized use. The User ID and</td>
<td>0007:0019</td>
</tr>
<tr>
<td>to protect their individual User ID and</td>
<td>PASSWORD</td>
<td>manually to unlock their workstation.</td>
<td>0090:0147</td>
</tr>
<tr>
<td>Users will always need to enter their</td>
<td>PASSWORD</td>
<td>may result in the compromise of</td>
<td>0003:0024</td>
</tr>
<tr>
<td>accounts. A poorly chosen</td>
<td>PASSWORD</td>
<td>. Shared accounts are not permitted</td>
<td>0010:0015</td>
</tr>
<tr>
<td>An employee cannot use another person's</td>
<td>PASSWORD</td>
<td>. The confidentiality of this password</td>
<td>0016:0007</td>
</tr>
<tr>
<td>Computer</td>
<td>PASSWORD</td>
<td>. Users will not share their passwords</td>
<td>0008:0026</td>
</tr>
<tr>
<td>accordance with the County's Computer</td>
<td>PASSWORD</td>
<td>. Users will not share their passwords</td>
<td>0009:0027</td>
</tr>
<tr>
<td>or secure cabinet. Back-ups shall be</td>
<td>PASSWORD</td>
<td>(and/or other authentication mechanism)</td>
<td>0042:0045</td>
</tr>
<tr>
<td>protected. The Security Officer shall</td>
<td>PASSWORD</td>
<td>on any system that resides at any</td>
<td>0002:0005</td>
</tr>
<tr>
<td>by the human resources department</td>
<td>PASSWORD</td>
<td>- a secure combination of characters</td>
<td>0051:0023</td>
</tr>
<tr>
<td>of such information. The use of</td>
<td>PASSWORD</td>
<td>assignments. All systems containing</td>
<td>0030:0008</td>
</tr>
<tr>
<td>Periodic reminders shall address</td>
<td>PASSWORD</td>
<td>by the human resources department</td>
<td>0089:0012</td>
</tr>
<tr>
<td>number. The devices are used with a</td>
<td>PASSWORD</td>
<td>can be used again by the same user</td>
<td>0066:0004</td>
</tr>
<tr>
<td>user to enter a unique user ID and</td>
<td>PASSWORD</td>
<td>/code. The confidentiality of this</td>
<td>0029:0018</td>
</tr>
<tr>
<td>to enforce the rules relating to</td>
<td>PASSWORD</td>
<td>from unauthorized use. The User ID and</td>
<td>0007:0019</td>
</tr>
<tr>
<td>screensaver protected by a user-defined</td>
<td>PASSWORD</td>
<td>manually to unlock their workstation.</td>
<td>0090:0147</td>
</tr>
<tr>
<td>necessary user identification and</td>
<td>PASSWORD</td>
<td>or account even with permission</td>
<td>0061:0007</td>
</tr>
<tr>
<td>to access without notice: data,</td>
<td>PASSWORD</td>
<td>Policy. Keep passwords secure and do</td>
<td>0005:0014</td>
</tr>
<tr>
<td>and Emergency Services; cell phone and</td>
<td>PASSWORD</td>
<td>protected. The Security Officer shall</td>
<td>0037:0018</td>
</tr>
<tr>
<td>for call will be required to carry</td>
<td>PASSWORD</td>
<td>protection (i.e., not posted)</td>
<td>0011:0019</td>
</tr>
<tr>
<td>of harassment via email, telephone or</td>
<td>PASSWORD</td>
<td>protection or file permissions are</td>
<td>0091:0122</td>
</tr>
<tr>
<td>reply to the first attempt, please try</td>
<td>PASSWORD</td>
<td>security, malicious software, incident</td>
<td>0035:0022</td>
</tr>
<tr>
<td>immediately, consider phoning or</td>
<td>PASSWORD</td>
<td>to establish authentication of users</td>
<td>0067:0011</td>
</tr>
<tr>
<td>Slacks, Jeans,</td>
<td>PART-TIME</td>
<td>to gain access. Sedgwick County may</td>
<td>0040:0017</td>
</tr>
<tr>
<td>on County employees, (full-time,</td>
<td>PART-TIME</td>
<td>usage found in the policy entitled</td>
<td>0045:0013</td>
</tr>
<tr>
<td>employees includes both full-time and</td>
<td>PART-TIME</td>
<td>will be used</td>
<td>0065:0052</td>
</tr>
<tr>
<td>3.7) Employees, contractors,</td>
<td>PART-TIME</td>
<td>program for purposes of identifying</td>
<td>0045:0015</td>
</tr>
<tr>
<td>attempts to obtain or distribute door</td>
<td>PASSCODES</td>
<td>attacks. Upon three (3) consecutive</td>
<td>0090:0148</td>
</tr>
<tr>
<td>to obtain or distribute door passcodes/</td>
<td>PASSKEYS</td>
<td>screen saver. (Must be disabled for</td>
<td>0003:0091</td>
</tr>
<tr>
<td>of your spouse or child is not a secure</td>
<td>PASSWORD</td>
<td>screensavers shall be installed on all</td>
<td>0042:0045</td>
</tr>
<tr>
<td>including assignment of username and</td>
<td>PASSWORD</td>
<td>The necessary user identification and</td>
<td>0009:0072</td>
</tr>
<tr>
<td>The necessary user identification and</td>
<td>PASSWORD</td>
<td>with security code, access code or</td>
<td>0008:0009</td>
</tr>
<tr>
<td>with security code, access code or</td>
<td>PASSWORD</td>
<td>be controlled by a secure username and</td>
<td>0008:0009</td>
</tr>
<tr>
<td>then provide a personalized Network</td>
<td>PASSWORD</td>
<td>then provide a personalized Network</td>
<td>0008:0026</td>
</tr>
<tr>
<td>identified with a unique username and</td>
<td>PASSWORD</td>
<td>identified with a unique username and</td>
<td>0010:0015</td>
</tr>
<tr>
<td>identified with a unique username and</td>
<td>PASSWORD</td>
<td>inactivity, the user must re-enter the</td>
<td>0010:0009</td>
</tr>
<tr>
<td>of access that supports or requires a</td>
<td>PASSWORD</td>
<td>with system security, menus and</td>
<td>0008:0009</td>
</tr>
<tr>
<td>with system security, menus and</td>
<td>PASSWORD</td>
<td>with system security, menus and</td>
<td>0008:0009</td>
</tr>
<tr>
<td>and the customer in his/her Microsoft</td>
<td>OUTLOOK</td>
<td>Calendar with a reminder that will</td>
<td>0095:0026</td>
</tr>
<tr>
<td>of Charleston County and current</td>
<td>OUTSOURCED</td>
<td>information technology vendor staff</td>
<td>0003:0406</td>
</tr>
<tr>
<td>of long-term goals and objectives for</td>
<td>OVERTIME</td>
<td>pay</td>
<td>0092:0036</td>
</tr>
<tr>
<td>to take time off instead of receiving</td>
<td>OVERTIME</td>
<td>rules will apply</td>
<td>0014:0033</td>
</tr>
<tr>
<td>off hours to resolve a problem, normal</td>
<td>OVERTIME</td>
<td>worked as a result of these procedures</td>
<td>0012:0006</td>
</tr>
</tbody>
</table>

KWIC INDEX TO GMIS POLICIES
KWIC INDEX TO GMIS POLICIES

<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>not limited to, system administration,</td>
<td>PASSWORDS</td>
<td>account management, and security</td>
<td>0063:0014</td>
</tr>
<tr>
<td>of user identification (user-ids),</td>
<td>PASSWORDS</td>
<td>and other network security standards</td>
<td>0053:0019</td>
</tr>
<tr>
<td>to prevent sharing of individual user</td>
<td>PASSWORDS</td>
<td>compromise of user rights</td>
<td>0065:0043</td>
</tr>
<tr>
<td>into the electronic mail system (i.e.,</td>
<td>PASSWORDS</td>
<td>encryption, etc.) to further protect</td>
<td>0016:0007</td>
</tr>
<tr>
<td>but not limited to: safeguarding their</td>
<td>PASSWORDS</td>
<td>maintaining reasonable physical</td>
<td>0002:0029</td>
</tr>
<tr>
<td>FORCE CRACK: A process of guessing</td>
<td>PASSWORDS</td>
<td>normally automated by a program, that</td>
<td>0066:0011</td>
</tr>
<tr>
<td>and up-to-date. All menu options,</td>
<td>PASSWORDS</td>
<td>operators and automatic setup routines</td>
<td>0026:0018</td>
</tr>
<tr>
<td>(hardware or software); compromised</td>
<td>PASSWORDS</td>
<td>tokens, or other means of controlled</td>
<td>0036:0013</td>
</tr>
<tr>
<td>using his/her access accounts or</td>
<td>PASSWORDS</td>
<td>Good judgment and safe computing</td>
<td>0091:0142</td>
</tr>
<tr>
<td>users with weak or non-conforming</td>
<td>PASSWORDS</td>
<td>Security staff shall promptly report</td>
<td>0045:0015</td>
</tr>
<tr>
<td>use vendor-supplied defaults for system</td>
<td>PASSWORDS</td>
<td>and other security parameters</td>
<td>0056:0008</td>
</tr>
<tr>
<td>4.1) Although confidential</td>
<td>PASSWORDS</td>
<td>are issued, users should be aware that</td>
<td>0004:0026</td>
</tr>
<tr>
<td>Unique User ID's and</td>
<td>PASSWORDS</td>
<td>are to use identified authorized users</td>
<td>0077:0004</td>
</tr>
<tr>
<td>Must have all</td>
<td>PASSWORDS</td>
<td>changed from the defaults</td>
<td>0080:0006</td>
</tr>
<tr>
<td>machine's hard disk drive and setting</td>
<td>PASSWORDS</td>
<td>for all applications and systems</td>
<td>0066:0134</td>
</tr>
<tr>
<td>should regularly change their user</td>
<td>PASSWORDS</td>
<td>for security purposes and are</td>
<td>0089:0012</td>
</tr>
<tr>
<td>are responsible for safeguarding their</td>
<td>PASSWORDS</td>
<td>for the system. Individual passwords</td>
<td>0001:0027</td>
</tr>
<tr>
<td>make all reasonable efforts to assure</td>
<td>PASSWORDS</td>
<td>are for the employees of their departments</td>
<td>0051:0007</td>
</tr>
<tr>
<td>to protect their individual user Id and</td>
<td>PASSWORDS</td>
<td>from unauthorized use. User Id's and</td>
<td>0071:0009</td>
</tr>
<tr>
<td>address the importance of confidential</td>
<td>PASSWORDS</td>
<td>in maintaining computer security, as</td>
<td>0035:0046</td>
</tr>
<tr>
<td>mobile devices shall have power-on</td>
<td>PASSWORDS</td>
<td>or data encryption to reduce the</td>
<td>0040:0029</td>
</tr>
<tr>
<td>their account and log-on information.</td>
<td>PASSWORDS</td>
<td>shall adhere to the following.</td>
<td>0050:0003</td>
</tr>
<tr>
<td>1.2.1</td>
<td>PASSWORDS</td>
<td>shall be maintained in accordance with</td>
<td>0005:0014</td>
</tr>
<tr>
<td>2. Computer and network</td>
<td>PASSWORDS</td>
<td>should not be shared. Each person must</td>
<td>0060:0011</td>
</tr>
<tr>
<td>To establish guidelines for all</td>
<td>PASSWORDS</td>
<td>that allow access to computer resources</td>
<td>0007:0003</td>
</tr>
<tr>
<td>not use encryption keys or encryption</td>
<td>PASSWORDS</td>
<td>that are unknown to their Department</td>
<td>0003:0131</td>
</tr>
<tr>
<td>are not permitted to encrypt or apply</td>
<td>PASSWORDS</td>
<td>to data unless it is for the purpose of</td>
<td>0068:0064</td>
</tr>
<tr>
<td>password. Users will not share their</td>
<td>PASSWORDS</td>
<td>with anyone under any circumstances.</td>
<td>0069:0027</td>
</tr>
<tr>
<td>in network design, lack of a current</td>
<td>PATCH</td>
<td>or other ways viruses and other</td>
<td>0032:0059</td>
</tr>
<tr>
<td>should have all</td>
<td>PATCH</td>
<td>Management Policy</td>
<td>0068:0321</td>
</tr>
<tr>
<td>4. Keep your Windows software *</td>
<td>PATCHED</td>
<td>all systems will be</td>
<td>0003:0229</td>
</tr>
<tr>
<td>* All systems will be</td>
<td>PATCHED</td>
<td>in accordance with industry best</td>
<td>0068:0323</td>
</tr>
<tr>
<td>will be patched with the most recent</td>
<td>PATCHES</td>
<td>at least once a quarter. Firewalls, web</td>
<td>0068:0323</td>
</tr>
<tr>
<td>efforts to notify Users when software</td>
<td>PATCHES</td>
<td>or other software is deployed to User</td>
<td>0003:0047</td>
</tr>
<tr>
<td>Application of</td>
<td>PATCHES</td>
<td>to operating systems and other</td>
<td>0087:0006</td>
</tr>
<tr>
<td>border devices will be evaluated for</td>
<td>PAYCHECK</td>
<td>on a quarterly basis</td>
<td>0068:0232</td>
</tr>
<tr>
<td>before receiving their final</td>
<td>PAYCHECKS</td>
<td>) they take the tape from the server and</td>
<td>0008:0086</td>
</tr>
<tr>
<td>RECEIVED FROM PAYROLL WITH</td>
<td>PAYDAY</td>
<td>* they take the tape from the server and</td>
<td>0075:0012</td>
</tr>
<tr>
<td>through Friday. Every other week (</td>
<td>PAYROLL</td>
<td>*</td>
<td>0092:0060</td>
</tr>
<tr>
<td>Kent County, or a subset thereof, i.e.</td>
<td>PAYROLL</td>
<td>, human resources. Though instances</td>
<td>0065:0010</td>
</tr>
<tr>
<td>and Alcohol, and SYS are in this class.</td>
<td>PAYROLL</td>
<td>personnel, and financial information</td>
<td>0068:0038</td>
</tr>
<tr>
<td>The weeks are identified as: 1 --</td>
<td>PAYROLL</td>
<td>Insurance</td>
<td>0106:0023</td>
</tr>
<tr>
<td>as a CSR, and filed through the normal</td>
<td>PAYROLL</td>
<td>1, 2 - Non-Payroll 1, 3 - Payroll 2, 4</td>
<td>0075:0005</td>
</tr>
<tr>
<td>as a CSR, and filed through the normal</td>
<td>PAYROLL</td>
<td>process by submitting hours to the</td>
<td>0012:0006</td>
</tr>
<tr>
<td>of their employment. Information for</td>
<td>PAYROLL</td>
<td>process by submitting hours to the</td>
<td>0019:0013</td>
</tr>
<tr>
<td>departments can include records such as</td>
<td>PAYROLL</td>
<td>purposes will be forwarded to the</td>
<td>0104:0014</td>
</tr>
<tr>
<td>be made to the employee in the form of</td>
<td>PAYROLL</td>
<td>sheet dupes, invoice dupes, agenda item</td>
<td>0008:0018</td>
</tr>
<tr>
<td>devices, whether County-owned or</td>
<td>PERSONALLY-OWNED</td>
<td>stipend</td>
<td>0011:0032</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>PHISHING</td>
<td>directly into the County</td>
<td>0065:0016</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>PHONORECORDS</td>
<td>equipment that is portable including</td>
<td>0059:0007</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>as defined by the Health Insurance</td>
<td>0069:0103</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>of County staff, banks, state agencies</td>
<td>0058:0019</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>, in which a work is fixed by any method</td>
<td>0058:0021</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>film, document or the like; to listen</td>
<td>0008:0040</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>and other still images, and motion</td>
<td>0058:0021</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>records and other data, information and</td>
<td>0057:0035</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>, and orders. It may also include</td>
<td>0008:0941</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>from magazines, books or other</td>
<td>0005:0025</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>is the unauthorized use of software</td>
<td>0058:0027</td>
</tr>
<tr>
<td>PERSONALLY-OWNED</td>
<td>Photograph</td>
<td>* or other software products that are</td>
<td>0005:0024</td>
</tr>
<tr>
<td>LEFT CONTEXT</td>
<td>KEYWORD</td>
<td>RIGHT CONTEXT</td>
<td>DOC:LINE</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>-Downloading or distributing</td>
<td>PIRATED</td>
<td>software or data.</td>
<td>0026:0011</td>
</tr>
<tr>
<td>knowingly to download or distribute</td>
<td>PIRATED</td>
<td>software or data.</td>
<td>0009:0206</td>
</tr>
<tr>
<td>or forwarding &quot;chain letters&quot;&quot;, &quot;</td>
<td>PONZI</td>
<td>&quot; or other &quot;pyramid&quot; schemes of any.</td>
<td>0005:0043</td>
</tr>
<tr>
<td>store, display, or request obscene,</td>
<td>PORNOGRAPHIC</td>
<td>erotic, profane, racist, sexist or.</td>
<td>0002:0038</td>
</tr>
<tr>
<td>??Accessing</td>
<td>PORNOGRAPHIC</td>
<td>material for other than law-enforcement</td>
<td>0052:0023</td>
</tr>
<tr>
<td>Accessing</td>
<td>PORNOGRAPHIC</td>
<td>material for other than law-enforcement</td>
<td>0054:0011</td>
</tr>
<tr>
<td>Policy, or that is of a sexual or</td>
<td>PORNOGRAPHIC</td>
<td>nature.</td>
<td>0069:0186</td>
</tr>
<tr>
<td>Village's Acceptable Use policy (e.g.,</td>
<td>PORNOGRAPHY</td>
<td>explicit content, racially-insensitive</td>
<td>0018:0021</td>
</tr>
<tr>
<td>disabilities, age, sexual orientation,</td>
<td>PORNOGRAPHY</td>
<td>religious beliefs and practice,</td>
<td>0003:0123</td>
</tr>
<tr>
<td>or threatening messages, gambling,</td>
<td>PORNOGRAPHY</td>
<td>viruses, chain letters, personal</td>
<td>0002:0007</td>
</tr>
<tr>
<td>1.2.2 Information contained on</td>
<td>PORTABLE</td>
<td>computers is especially vulnerable and.</td>
<td>0005:0016</td>
</tr>
<tr>
<td>DIGITAL ASSISTANTS (PDA): A family of</td>
<td>PORTABLE</td>
<td>devices offering personal productivity.</td>
<td>0065:0012</td>
</tr>
<tr>
<td>* Do not leave</td>
<td>PORTABLE</td>
<td>media such as CDs or floppy disks in.</td>
<td>0003:0284</td>
</tr>
<tr>
<td>County's PC's and servers, including</td>
<td>PORTABLE</td>
<td>, to ensure that Sedgwick County is in...</td>
<td>0058:0056</td>
</tr>
<tr>
<td>Office Professional (Word, Excel,</td>
<td>POWERPOINT</td>
<td>, Ol. look...</td>
<td>0002:0294</td>
</tr>
<tr>
<td>&quot;H&quot; drive documents (Word, Excel and</td>
<td>POWERPOINT</td>
<td>) to the department's shared folder in a...</td>
<td>0088:0019</td>
</tr>
<tr>
<td>Microsoft</td>
<td>POWERPOINT</td>
<td>2002 &amp; PowerPoint 2000.</td>
<td>0090:0075</td>
</tr>
<tr>
<td>Allow worker productivity and (b) does not</td>
<td>PREEMPT</td>
<td>any County business activity.</td>
<td>0083:0070</td>
</tr>
<tr>
<td>The Kansas Government Records</td>
<td>PRESERVATION</td>
<td>Act charges counties with the.</td>
<td>0057:0004</td>
</tr>
<tr>
<td>counties with the responsibility to</td>
<td>PRESERVE</td>
<td>&quot;records with enduring value,&quot; to.</td>
<td>0057:0004</td>
</tr>
<tr>
<td>agent for this Policy/Procedure and to</td>
<td>PRESERVE</td>
<td>and protect those confidential rights...</td>
<td>0041:015</td>
</tr>
<tr>
<td>environmental reports, PAMP (</td>
<td>PRESERVE</td>
<td>area management plan), meeting minutes</td>
<td>0008:0566</td>
</tr>
<tr>
<td>7. Collect and</td>
<td>PRESERVE</td>
<td>evidence...</td>
<td>0068:0225</td>
</tr>
<tr>
<td>userid and request to capture and</td>
<td>PRESERVE</td>
<td>the employee's computer or other...</td>
<td>0054:0015</td>
</tr>
<tr>
<td>user privileges when necessary to</td>
<td>PRESERVE</td>
<td>the integrity, confidentiality, and...</td>
<td>0040:0017</td>
</tr>
<tr>
<td>as determined to be appropriate, to</td>
<td>PRESERVE</td>
<td>the integrity of data...</td>
<td>0044:0014</td>
</tr>
<tr>
<td>to civil and criminal process. To</td>
<td>PRESERVE</td>
<td>the security and availability of Gaston...</td>
<td>0002:0011</td>
</tr>
<tr>
<td>including review of captured and</td>
<td>PRESERVED</td>
<td>computer history. Committee members...</td>
<td>0054:0016</td>
</tr>
<tr>
<td>to) [&quot;published material acquired and</td>
<td>PRESERVED</td>
<td>solely for reference purposes, extra...</td>
<td>0057:0037</td>
</tr>
<tr>
<td>records, with particular attention to</td>
<td>PRESERVING</td>
<td>those records that document Sedgwick...</td>
<td>0057:0019</td>
</tr>
<tr>
<td>the tone, enter your phone number and</td>
<td>PRESS</td>
<td>the pound (#) symbol. Or you can send a...</td>
<td>0019:0004</td>
</tr>
<tr>
<td>1.</td>
<td>PRESS</td>
<td>the telephone line button for extension...</td>
<td>0097:0044</td>
</tr>
<tr>
<td>- Internet providers, America On-Line,</td>
<td>PRODIGY</td>
<td>; provided however, that any...</td>
<td>0015:0005</td>
</tr>
<tr>
<td>harassing, embarrassing, indecent,</td>
<td>PROFANE</td>
<td>, CompuServe, etc...</td>
<td>0051:0013</td>
</tr>
<tr>
<td>request obscene, pornographic, erotic,</td>
<td>PROFANE</td>
<td>obscene, intimidating, or other...</td>
<td>0001:0023</td>
</tr>
<tr>
<td>in a way which includes the use of</td>
<td>PROFANE</td>
<td>racist, sexist or offensive.</td>
<td>0002:0028</td>
</tr>
<tr>
<td>upon the rights of others. No abusive,</td>
<td>PROFANE</td>
<td>offensive language or, in the...</td>
<td>0040:0023</td>
</tr>
<tr>
<td>of licenses issued to business,</td>
<td>PROFANE</td>
<td>offensive language is transmitted...</td>
<td>0061:0009</td>
</tr>
<tr>
<td>Windows XP</td>
<td>PROFessional</td>
<td>, or occupation within &quot;local governing...</td>
<td>0008:0664</td>
</tr>
<tr>
<td>* Microsoft Office</td>
<td>PROFessional</td>
<td>(CAL)</td>
<td>0090:0067</td>
</tr>
<tr>
<td>with changes in the law, regulations,</td>
<td>PROFessional</td>
<td>in content and purpose...</td>
<td>0002:0053</td>
</tr>
<tr>
<td>with changes in the law, regulations,</td>
<td>PROFessional</td>
<td>in nature. The use of these systems...</td>
<td>0069:0174</td>
</tr>
<tr>
<td>that electronic communication is</td>
<td>PROFessional</td>
<td>integrity. Your job duties may require...</td>
<td>0059:0007</td>
</tr>
<tr>
<td>County. All communications should be</td>
<td>PROFessional</td>
<td>manner, respectful of others and the...</td>
<td>0065:0022</td>
</tr>
<tr>
<td>of special trust and reliance on your</td>
<td>PROFessional</td>
<td>reasons. Employees are responsible for...</td>
<td>0061:0005</td>
</tr>
<tr>
<td>are expected to conduct themselves in a</td>
<td>PROFessional</td>
<td>training...</td>
<td>0091:0078</td>
</tr>
<tr>
<td>All communications shall be for</td>
<td>PROFessional</td>
<td>professionalism within the City of Montgomery, past...</td>
<td>0092:0027</td>
</tr>
<tr>
<td>* On-line computer or</td>
<td>PROFessional</td>
<td>and be customer focused - to our...</td>
<td>0003:0037</td>
</tr>
<tr>
<td>require substantial creative work by a</td>
<td>PROFessional</td>
<td>of Sedgwick County. Content should pass...</td>
<td>0053:0012</td>
</tr>
<tr>
<td>Technology Services will demonstrate</td>
<td>PROFessional</td>
<td>in the workplace and to refrain from...</td>
<td>0091:0090</td>
</tr>
<tr>
<td>good judgment and reflect the</td>
<td>PYRAMID</td>
<td>&quot; schemes of any type...</td>
<td>0005:0043</td>
</tr>
<tr>
<td>are expected to conduct themselves</td>
<td>QUICKEN</td>
<td>&quot; , Publisher, Print Shop, etc...</td>
<td>0090:0231</td>
</tr>
<tr>
<td>&quot;chain letters&quot;, &quot;Ponzi&quot; or other &quot;</td>
<td>RACE</td>
<td>color, sex, religion, creed, national...</td>
<td>0040:0023</td>
</tr>
<tr>
<td>single user programs. (Examples are:</td>
<td>RACE</td>
<td>color, religion, national origin, age...</td>
<td>0069:0199</td>
</tr>
<tr>
<td>work environment based on his/her</td>
<td>RACE</td>
<td>gender, disabilities, age, sexual...</td>
<td>0002:0057</td>
</tr>
<tr>
<td>offensive material on the basis of sex,</td>
<td>RACE</td>
<td>gender, color, disabilities, age...</td>
<td>0003:0123</td>
</tr>
<tr>
<td>including offensive comments about</td>
<td>RACE</td>
<td>, religion, national origin, physical...</td>
<td>0061:0015</td>
</tr>
</tbody>
</table>
to another on the basis of sex, race, ethnicity, age, disability, age, or national origin. 

Race, religion, color, national origin, sex, age, or national origin. 

Race, religion, color, national origin, sex, age, or national origin. 

Race, religion, color, national origin, sex, age, or national origin. 

Racially insensitive, religious, threatening. 

Racially insensitive, religious, threatening. 

Racially insensitive, religious, threatening. 

Racially insensitive, religious, threatening. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher or for an employee of the County. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher. 

Software publisher. Software must be registered in the name of Sedgwick County and the software publisher.
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>privileges and/or have their contracts</td>
<td>REVOKED</td>
<td>Additional legal remedies may also be...........0005:0129</td>
<td></td>
</tr>
<tr>
<td>system and/or have their contract procedures may have their contract</td>
<td>REVOKED</td>
<td>Other legal remedies, including.............0003:0277</td>
<td></td>
</tr>
<tr>
<td>11. All access for a user ID will be</td>
<td>REVOKED</td>
<td>after a specified period of no use. The........0090:0137</td>
<td></td>
</tr>
<tr>
<td>is a privilege, not a right, and may be</td>
<td>REVOKED</td>
<td>at any time for use inconsistent with...........0062:0008</td>
<td></td>
</tr>
<tr>
<td>a privilege, not a right, which may be</td>
<td>REVOKED</td>
<td>at any time. The County retains the.............0064:0006</td>
<td></td>
</tr>
<tr>
<td>system is a privilege that may be</td>
<td>REVOKED</td>
<td>at any time. ......................................0069:0188</td>
<td></td>
</tr>
<tr>
<td>a right. As such, the privilege may be</td>
<td>REVOKED</td>
<td>at any time and for any reason. Limited........0083:0070</td>
<td></td>
</tr>
<tr>
<td>access for non-City purposes may be</td>
<td>REVOKED</td>
<td>or limited at any time by appropriate...........0091:0087</td>
<td></td>
</tr>
<tr>
<td>each user every year. Keys shall be</td>
<td>REVOKING</td>
<td>upon termination, change in job.................0042:0061</td>
<td></td>
</tr>
<tr>
<td>code), the DSA shall be responsible for</td>
<td>SANDALS</td>
<td>such access immediately upon completion0039:0074</td>
<td></td>
</tr>
<tr>
<td>* Loafers, boots, dress shoes, dress</td>
<td>E.</td>
<td>TOKENS: A small device that displays a..........0005:0027</td>
<td></td>
</tr>
<tr>
<td>whenever possible through the use of</td>
<td>SECUREID</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>Intranet - The County network and maintain a user list on each file</td>
<td>K. REMOTE ACCESS</td>
<td>This device routes suspicious e-mail............0076:0021</td>
<td></td>
</tr>
<tr>
<td>it is allowed to enter the e-mail</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>malicious programs into the network or</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>common known as AS/400 is a midrange</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>G. Central</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>will be retained on the County's e-mail</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>policy to move to a 100% Microsoft</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>Such procedures shall identify the</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>and offensive messages received.</td>
<td>SERVER</td>
<td>(e.g., viruses, worms, Trojan horses............0005:0027</td>
<td></td>
</tr>
<tr>
<td>may be stored temporarily on the</td>
<td>SERVER'S</td>
<td>backup system..................................0004:0051</td>
<td></td>
</tr>
<tr>
<td>Gaston County PCs, PDAs, smart phones, of all Sedgwick County's PC's and</td>
<td>SERVERS</td>
<td>, including portables, to ensure that...........0058:0056</td>
<td></td>
</tr>
<tr>
<td>will be stored on network directories on local area network to the following: host computers, file devices including, but not limited to,</td>
<td>SERVERS</td>
<td>, not on individual workstations. This...........0065:0043</td>
<td></td>
</tr>
<tr>
<td>a department, on the Town's</td>
<td>SERVERS</td>
<td>, or other mechanisms. .........................0090:0163</td>
<td></td>
</tr>
<tr>
<td>used in order to recover passwords on</td>
<td>SERVERS</td>
<td>, workstations, stand-alone computers........0001:0018</td>
<td></td>
</tr>
<tr>
<td>County data is stored on county file</td>
<td>SERVERS</td>
<td>workstations, and external connections........0005:0156</td>
<td></td>
</tr>
<tr>
<td>(e.g., relocating workstations or</td>
<td>SERVERS</td>
<td>workstations, and external connections........0005:0156</td>
<td></td>
</tr>
<tr>
<td>our network must pass through company</td>
<td>SERVERS</td>
<td>workstations, and external connections........0005:0156</td>
<td></td>
</tr>
<tr>
<td>Network The Network</td>
<td>SERVERS</td>
<td>workstations, and external connections........0005:0156</td>
<td></td>
</tr>
<tr>
<td>zone) with the application and database</td>
<td>SERVERS</td>
<td>workstations, and external connections........0005:0156</td>
<td></td>
</tr>
<tr>
<td>pornographic, erotic, profane, racist, content, derogatory religious content, material that is in violation of the City, including but not limited to, that would violate the County's</td>
<td>SEXIST</td>
<td>or other offensive material (including............0002:0038</td>
<td></td>
</tr>
<tr>
<td>F.7.a. SEXUAL Harassment: Violating federal, state</td>
<td>SEXUAL</td>
<td>content, political statements....................0061:0009</td>
<td></td>
</tr>
<tr>
<td>will be retained on the County's e-mail</td>
<td>SEXUAL</td>
<td>“harassment or hostile workplace policy........0005:0029</td>
<td></td>
</tr>
<tr>
<td>policy to move to a 100% Microsoft</td>
<td>SEXUAL</td>
<td>&quot;harassment, shall be reported following........0091:0127</td>
<td></td>
</tr>
<tr>
<td>Such procedures shall identify the</td>
<td>SEXUAL</td>
<td>&quot;harassment Policy, or that is of a ..........0069:0186</td>
<td></td>
</tr>
<tr>
<td>and offensive messages received.</td>
<td>SEXUAL</td>
<td>&quot;Harassment: Violating federal, state ..........0065:0036</td>
<td></td>
</tr>
<tr>
<td>may be stored temporarily on the</td>
<td>SEXUAL</td>
<td>implications, racial slurs, gender.............0004:0034</td>
<td></td>
</tr>
<tr>
<td>Gaston County PCs, PDAs, smart phones, of all Sedgwick County's PC's and</td>
<td>SEXUAL</td>
<td>implications, racial slurs, gender.............0004:0034</td>
<td></td>
</tr>
<tr>
<td>will be stored on network directories on local area network to the following: host computers, file devices including, but not limited to,</td>
<td>SEXUAL</td>
<td>implications, racial slurs, gender.............0004:0034</td>
<td></td>
</tr>
</tbody>
</table>
| 4/7/2008 Page 290 of 296
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>storing, copying, or transmission of</td>
<td>SEXUALLY explicit or sexually oriented materials</td>
<td>...0091.0092</td>
<td></td>
</tr>
<tr>
<td>into the following categories: adult/</td>
<td>SEXUALLY explicit, violence, criminal skills,</td>
<td>...0065.0013</td>
<td></td>
</tr>
<tr>
<td>Adult/</td>
<td>Explicit</td>
<td>...0082.0015</td>
<td></td>
</tr>
<tr>
<td>Keep passwords secure and do not</td>
<td>SHARE accounts. Authorized users are</td>
<td>...0005.0014</td>
<td></td>
</tr>
<tr>
<td>utilizing the Village Network</td>
<td>common disk drives and therefore</td>
<td>...0026.0003</td>
<td></td>
</tr>
<tr>
<td>Schaumburg and those who work with or</td>
<td>SHARE common membership in organizations</td>
<td>...0031.0014</td>
<td></td>
</tr>
<tr>
<td>entire workgroups or departments to</td>
<td>SHARE data. Requests for special workgroups</td>
<td>...0068.0093</td>
<td></td>
</tr>
<tr>
<td>to the inability to easily exchange or</td>
<td>SHARE documents and effectively send and</td>
<td>...0090.0023</td>
<td></td>
</tr>
<tr>
<td>Do not</td>
<td>SHARE Gaston County passwords with anyone</td>
<td>...0002.0197</td>
<td></td>
</tr>
<tr>
<td>4.3) Users should not</td>
<td>SHARE their passwords with anyone</td>
<td>...0007.0009</td>
<td></td>
</tr>
<tr>
<td>confidentiality users should not</td>
<td>SHARE their passwords with anyone under any</td>
<td>...0069.0027</td>
<td></td>
</tr>
<tr>
<td>username and password. Users will not</td>
<td>SHARE your knowledge and abilities with</td>
<td>...0001.0036</td>
<td></td>
</tr>
<tr>
<td>develop your computer use skills and to</td>
<td>SHARE accounts are not permitted</td>
<td>...0105.0015</td>
<td></td>
</tr>
<tr>
<td>and network passwords should not be</td>
<td>SHARE between the Village and the service</td>
<td>...0015.0003</td>
<td></td>
</tr>
<tr>
<td>by a secure username and password.</td>
<td>SHARE computer system shall be secure and</td>
<td>...0051.0036</td>
<td></td>
</tr>
<tr>
<td>of the responsibilities being</td>
<td>SHARE County records storage facilities</td>
<td>...0057.0076</td>
<td></td>
</tr>
<tr>
<td>client department's information in a</td>
<td>SHARE department drive</td>
<td>...0088.0008</td>
<td></td>
</tr>
<tr>
<td>divisional / departmental or</td>
<td>SHARE drives</td>
<td>...0005.0064</td>
<td></td>
</tr>
<tr>
<td>personal folder (H drive) from the</td>
<td>SHARE information such as; Policies, HR</td>
<td>...0085.0010</td>
<td></td>
</tr>
<tr>
<td>recommends saving all data to network/</td>
<td>SHARE Key Encryption set</td>
<td>...0080.0007</td>
<td></td>
</tr>
<tr>
<td>* Must have a minimum of 46-bit</td>
<td>SHARE or revealed to anyone else besides the</td>
<td>...0090.0016</td>
<td></td>
</tr>
<tr>
<td>network... A VPN works by using the</td>
<td>SHARE public infrastructure while maintaining</td>
<td>...0092.0263</td>
<td></td>
</tr>
<tr>
<td>shows restraint in the consumption of</td>
<td>SHARE resources. It demonstrates respect for</td>
<td>...0091.0043</td>
<td></td>
</tr>
<tr>
<td>shows restraint in the consumption of</td>
<td>SHARE resources. Users shall refrain from</td>
<td>...0003.0081</td>
<td></td>
</tr>
<tr>
<td>assigned access to any folders or other</td>
<td>SHARE server resources</td>
<td>...0068.0087</td>
<td></td>
</tr>
<tr>
<td>3. Generic or</td>
<td>SHARE user IDs shall not be utilized under</td>
<td>...0042.0031</td>
<td></td>
</tr>
<tr>
<td>User Id's and passwords are not to be</td>
<td>SHARE with any other person</td>
<td>...0071.0009</td>
<td></td>
</tr>
<tr>
<td>User ID and passwords are not to be</td>
<td>SHARE with anyone. Employees are expected to</td>
<td>...0077.0006</td>
<td></td>
</tr>
<tr>
<td>user and should not be provided to or</td>
<td>SHARE with coworkers, supervisors, or other</td>
<td>...0065.0051</td>
<td></td>
</tr>
<tr>
<td>programs downloaded from the Internet</td>
<td>SHAREWARE &quot;freeware,&quot; scripts, or applet</td>
<td>...0065.0033</td>
<td></td>
</tr>
<tr>
<td>of this software, called &quot;freeware&quot; or</td>
<td>SHAREWARE &quot;is available free of charge for</td>
<td>...0090.0084</td>
<td></td>
</tr>
<tr>
<td>software, including &quot;freeware&quot; and/or</td>
<td>SHAREWARE &quot;programs unless previously approved.</td>
<td>...0003.0137</td>
<td></td>
</tr>
<tr>
<td>* The copyright holders for</td>
<td>SHAREWARE allow purchasers to make and distribute</td>
<td>...0005.0033</td>
<td></td>
</tr>
<tr>
<td>* Using unlicensed software, or using</td>
<td>SHAREWARE beyond its evaluation period</td>
<td>...0091.0010</td>
<td></td>
</tr>
<tr>
<td>* Never download freeware or</td>
<td>SHAREWARE from the Internet without express</td>
<td>...0076.0033</td>
<td></td>
</tr>
<tr>
<td>of such material or downloading</td>
<td>SHAREWARE may not be undertaken without express</td>
<td>...0002.0003</td>
<td></td>
</tr>
<tr>
<td>systems. Identify freeware or</td>
<td>SHAREWARE or purchase software to conduct such a</td>
<td>...0032.0061</td>
<td></td>
</tr>
<tr>
<td>Messaging and Peer to Peer File</td>
<td>SHARING</td>
<td>...0081.0001</td>
<td></td>
</tr>
<tr>
<td>* Peer-to-peer file</td>
<td>SHARING</td>
<td>...0092.0223</td>
<td></td>
</tr>
<tr>
<td>* Peer-to-peer file</td>
<td>SHARING</td>
<td>...0096.0054</td>
<td></td>
</tr>
<tr>
<td>telnet, browsing, file and print</td>
<td>SHARING</td>
<td>...0065.0014</td>
<td></td>
</tr>
<tr>
<td>* Enable ease of obtaining and</td>
<td>SHARING</td>
<td>...0091.0064</td>
<td></td>
</tr>
<tr>
<td>personnel, and the appropriate</td>
<td>SHARING</td>
<td>...0003.0028</td>
<td></td>
</tr>
<tr>
<td>16.3.20 Dress</td>
<td>SHARING</td>
<td>...0060.0074</td>
<td></td>
</tr>
<tr>
<td>INTO THE FOLLOWING CATEGORIES: adult/</td>
<td>SHIRTS Tops, Blouses, and Jackets</td>
<td>...0100.0009</td>
<td></td>
</tr>
<tr>
<td>SHIRTS and Footwear</td>
<td>SHOES</td>
<td>...0100.0025</td>
<td></td>
</tr>
<tr>
<td>SHOP,</td>
<td>SHOPPING</td>
<td>...0009.0023</td>
<td></td>
</tr>
<tr>
<td>viruses, chain letters, personal</td>
<td>SHOPPING, executable 'ready to run files'</td>
<td>...0002.0007</td>
<td></td>
</tr>
<tr>
<td>does not include use for the purpose of</td>
<td>SHOPPING, gambling, gaming, nor do you express</td>
<td>...0005.0033</td>
<td></td>
</tr>
<tr>
<td>while taking three hours to go</td>
<td>SHOPPING at the mall during the workday is not</td>
<td>...0003.0102</td>
<td></td>
</tr>
<tr>
<td>* Confidential information may be</td>
<td>SHREDDED prior to recycling, if recommended by</td>
<td>...0057.0010</td>
<td></td>
</tr>
<tr>
<td>SHREDDED to those who really need the</td>
<td>SKIRTS Dresses, and Skirted Suits</td>
<td>...0100.0121</td>
<td></td>
</tr>
<tr>
<td>SLIPERS are unacceptable</td>
<td>SLIPERS used to balance for cash deposits. See</td>
<td>...0008.0147</td>
<td></td>
</tr>
<tr>
<td>SLIPERS, unless authorized in writing in</td>
<td>SNIPPERS, pinged floods, packet spoofing, denial</td>
<td>...0005.0031</td>
<td></td>
</tr>
<tr>
<td>non-essential functionalities (SMTP,</td>
<td>FTP). FTP or any other access is</td>
<td>...0003.0189</td>
<td></td>
</tr>
<tr>
<td>LEFT CONTEXT</td>
<td>KEYWORD</td>
<td>RIGHT CONTEXT</td>
<td>DOC:LINE</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>attacks, e.g., eavesdropping,醍醐</td>
<td>SNOOPING</td>
<td>are prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>mail and other forms of electronic</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>ELECTRONIC RECORDS</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>5: Use and regularly update anti-virus</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>4. Computer</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>stand-alone computers, laptops,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>setup equipment, peripheral,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>Sedgwick County implements hardware,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>Information assets including hardware,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>including computing equipment,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>data files, programs, application</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>e.g., addition of new hardware or</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>and related peripheral equipment and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>different versions of operating system</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>is not limited to, computer equipment,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>County has made in computer hardware,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>compatible with such hardware and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>storage logs and records management</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>5. Install needed Application</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>printers, scanners, mobile devices) and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>technology requirements (hardware and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>following: property theft (hardware or</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>the responsibility for all computers,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>of Information Technology created</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>Requests for Customized</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>5. To prevent programming or</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>and that basic business productivity</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>small technology Commodity Hardware and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>Backups are done using the native</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>funded; the computer systems and the</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>D. Configuration, Maintenance,</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>intellectual property, such as</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>4.b.</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>a log, left with the computer, of all</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>5. Only approved</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>will use commercially available</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>adopted a Personal Computer</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>Information Processing: Accessing</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>allow access only to those persons or</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>SOFTWARE programs that have been granted access.</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>B. Requesting routine installation of</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>B. Requesting routine installation of</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>apply to all technology hardware and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>2.3. Contain virus-checking</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>will provide the synchronization</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>proper authorization or use hardware</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>but are not limited to: computer</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>workstations or servers), all e-PHI and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>5. Wireless adaptor</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>2) IT has authorized the</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>viruses and</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>2) IT has authorized the</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>as it can result in the increase of</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>objectionable, unsolicited material</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>request such material (email</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>send a copy of the email to the email</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
<tr>
<td>Bermuda shorts, leggings, and any</td>
<td>SOFTWARE</td>
<td>prohibited. The County will not</td>
<td>0053:0024</td>
</tr>
</tbody>
</table>

4/7/2008 Page 292 of 296
TELECOMMUNICATIONS Policies And Procedures

1. DIO/IT Networking & TELECOMMUNICATIONS shall assign unique user identification...0042:0027

2. The BOCC may agree to pay a cell phone STIPEND for a cell phone package purchased by...0011:0003

3. Telecommunication charges...0060:0033

4. All backup TAPE or disks from any system should be...0060:0033

5. Tapes are maintained in a Compaq StorageWorks SSL 2020 Tape Library Unit. Tapes will be...0075:0008

6. The BOCC may agree to pay a cell phone STIPEND for a cell phone package purchased by...0011:0003
### KWIC INDEX TO GMIS POLICIES

<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
<th>DOC:LINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>systems equipment, power sources,</td>
<td>TELEPHONE</td>
<td>jacks and other telecommunications</td>
<td>0039:0062</td>
</tr>
<tr>
<td>processing equipment connected to any</td>
<td>TELEPHONE</td>
<td>line or network belonging to, or</td>
<td>0091:0014</td>
</tr>
<tr>
<td>processing equipment connected to any</td>
<td>TELEPHONE</td>
<td>...</td>
<td>0091:0014</td>
</tr>
<tr>
<td>information (i.e. mission statement,</td>
<td>TELEPHONE</td>
<td>list, map/directions, employee</td>
<td>0008:0221</td>
</tr>
<tr>
<td>of credible virus threats via e-mail or</td>
<td>TELEPHONE</td>
<td>messages. Because this notification</td>
<td>0076:0029</td>
</tr>
<tr>
<td>to the Internet. The Public Switched</td>
<td>TELEPHONE</td>
<td>Network is considered to be a secure</td>
<td>0068:0062</td>
</tr>
<tr>
<td>of regular business hours by means of</td>
<td>TELEPHONE</td>
<td>number (334) 241-2149</td>
<td>0097:0007</td>
</tr>
<tr>
<td>f.</td>
<td>TELEPHONE</td>
<td>number (direct if possible)</td>
<td>0085:0026</td>
</tr>
<tr>
<td>may also capture User Activity such as</td>
<td>TELEPHONE</td>
<td>numbers and/or e-mail addresses for all</td>
<td>0037:0051</td>
</tr>
<tr>
<td>notify the Security Officer by</td>
<td>TELEPHONE</td>
<td>in person. To the fullest extent</td>
<td>0036:0018</td>
</tr>
<tr>
<td>the functional equivalent of informal</td>
<td>TELEPHONE</td>
<td>such as in-person conversations, which do</td>
<td>0057:0130</td>
</tr>
<tr>
<td>2. Any form of harassment via email,</td>
<td>TELEPHONE</td>
<td>or paging, whether through language</td>
<td>0005:0040</td>
</tr>
<tr>
<td>in a matter of minutes over the</td>
<td>TELEPHONE</td>
<td>or with Remote Desktop Tools by a</td>
<td>0095:0019</td>
</tr>
<tr>
<td>must be completed. Forms for</td>
<td>TELEPHONE</td>
<td>reference checks can be found on the</td>
<td>0104:0008</td>
</tr>
<tr>
<td>the server and store it off site in our</td>
<td>TELEPHONE</td>
<td>safe at city hall. The tape from the</td>
<td>0001:0012</td>
</tr>
<tr>
<td>2.6.1 allows for storage of that individual's</td>
<td>TELEPHONE</td>
<td>Usage</td>
<td>0002:0097</td>
</tr>
<tr>
<td>dial-up lines, private networks, and</td>
<td>TELEPHONE</td>
<td>voice mail. The user will access</td>
<td>0029:0018</td>
</tr>
<tr>
<td>Cellular</td>
<td>TELEPHONE</td>
<td>voice response and &quot;faxback&quot; systems</td>
<td>0046:0005</td>
</tr>
<tr>
<td>Gaston County provides its staff with</td>
<td>TELEPHONES</td>
<td>telephones for conducting official county</td>
<td>0001:0001</td>
</tr>
<tr>
<td>1. Carry their assigned mobile</td>
<td>TELEPHONES</td>
<td>clients; desktop, laptop and notebook</td>
<td>0040:0013</td>
</tr>
<tr>
<td>electronic mail, Internet access,</td>
<td>TELEPHONES</td>
<td>, browsing, file and print sharing</td>
<td>0065:0014</td>
</tr>
<tr>
<td>is not limited to, &quot;dumb terminals&quot;; &quot;</td>
<td>TIME-AND-A-HALF</td>
<td>pay will begin once a cumulative hourly</td>
<td>0019:0011</td>
</tr>
<tr>
<td>* Work boots, dirty athletic shoes,</td>
<td>TIME-AND-A-HALF</td>
<td>along with any required documentation</td>
<td>0008:0006</td>
</tr>
<tr>
<td>assistants (PDAs), and USB drives (or</td>
<td>TIME-AND-A-HALF</td>
<td>before the computers are automatically</td>
<td>0000:0013</td>
</tr>
<tr>
<td>receive a minimum of two hours pay.</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>leave of absences, time sheets or</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>should define a maximum inactivity</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>using e-PHI shall employ inactivity</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>Drugs, Alcohol, &amp;</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>The types of drills include: fire,</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>to, major storms, floods, fires,</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>human error; and acts of God (e.g.,</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>a backup, the problem will be logged in</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>8. Follow up and update</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>corporate credit cards, petty cash, and</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>receiving reports, refund requests,</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>does not compensate staff members for</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>does not compensate staff members for</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>Technology business, to include</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>1. All information</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>or may have light usage, but frequently</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>may contain viruses, e-mail bombs, or</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>or propagating any virus, worm,</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>of computer viruses: true viruses,</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>non-business-related messages to</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>a system of user identification (</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>User identifier (</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>temporarily deactivate the employee's</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>use any part of the account identifier (</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>be uniquely identified with a unique</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>be uniquely identified with a unique</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>on the system, including assignment of</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>Access will be controlled by a secure</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>and Root level passwords and data, pager memory banks, email and</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>of job description used to fill job</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>a password to co-workers while on</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>if employees are on leave of absence,</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
<tr>
<td>also consists of the leave balances of</td>
<td>TIME-AND-A-HALF</td>
<td>...</td>
<td>0000:0013</td>
</tr>
</tbody>
</table>

---

4/7/2008 Page 294 of 296
<table>
<thead>
<tr>
<th>LEFT CONTEXT</th>
<th>KEYWORD</th>
<th>RIGHT CONTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>be determined by availability, meaning VACATIONS and other time off, will be considered.</td>
<td>...0014:0036</td>
<td></td>
</tr>
<tr>
<td>violation notices, tag receipts, rabies VACCINATIONS certificates, neglect or abuse cases</td>
<td>...0008:0461</td>
<td></td>
</tr>
<tr>
<td>eavesdropping, snooping, fraud, theft, VANDALISM, sabotage, blackmail</td>
<td>...0032:0051</td>
<td></td>
</tr>
<tr>
<td>or other occurrence (e.g., fire, VANDALISM, system failure, natural disaster)</td>
<td>...0037:0006</td>
<td></td>
</tr>
<tr>
<td>well as protect against data theft or VANDALISM from outside sources</td>
<td>...0002:0233</td>
<td></td>
</tr>
<tr>
<td>secure from damage due to tampering, VANDALS who exploit weaknesses in these</td>
<td>...0002:0073</td>
<td></td>
</tr>
<tr>
<td>activity on the part of hackers and VAX 3800 Minicomputers, Accounting and</td>
<td>...0068:0154</td>
<td></td>
</tr>
<tr>
<td>CLIENT CASE FILES: qualified applicants who are claiming VETERAN'S Preference (FS 295.07)</td>
<td>...0010:0047</td>
<td></td>
</tr>
<tr>
<td>as all originals are forwarded to the VETERANS Administration for processing.</td>
<td>...0008:0454</td>
<td></td>
</tr>
<tr>
<td>the same regardless of the medium, paper, VOICE, and telecommunication technology</td>
<td>...0069:0224</td>
<td></td>
</tr>
<tr>
<td>or local ordinances. Electronic and VOICE mail capabilities provided to employees</td>
<td>...0051:0008</td>
<td></td>
</tr>
<tr>
<td>from working, the user should leave a VOICE mail on the Banner hotline, if</td>
<td>...0057:0132</td>
<td></td>
</tr>
<tr>
<td>or no administrative value, Internet access, electronic mail and</td>
<td>...0029:0002</td>
<td></td>
</tr>
<tr>
<td>Internet access, electronic and VOICE mail, self-sticking notes, and</td>
<td>...0034:0011</td>
<td></td>
</tr>
<tr>
<td>to working, the user should leave a VOICE mail on the Banner hotline, if</td>
<td>...0014:0008</td>
<td></td>
</tr>
<tr>
<td>or no administrative value, Internet access, electronic and</td>
<td>...0029:0002</td>
<td></td>
</tr>
<tr>
<td>Internet access, electronic and to an individual's (1) electronic or</td>
<td>...0057:0132</td>
<td></td>
</tr>
<tr>
<td>lines, private networks, and telephone via the computer rather than using</td>
<td>...0057:0132</td>
<td></td>
</tr>
<tr>
<td>accounts providing electronic mail, the employee is Town Hall based their</td>
<td>...0057:0132</td>
<td></td>
</tr>
<tr>
<td>their departmental, e-mail and 2.6 Phone and</td>
<td>...0057:0132</td>
<td></td>
</tr>
<tr>
<td>this stipend will be included on my Microsoft Windows platform (</td>
<td>...0057:0132</td>
<td></td>
</tr>
<tr>
<td>2.6 Phone and this stipend will be included on my Microsoft Windows platform (</td>
<td>...0057:0132</td>
<td></td>
</tr>
<tr>
<td>Gaming: betting, gambling, WAGERING</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>Gaming: betting, gambling, 4. Use technology resources for</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>related to illegal gambling, illegal WAGERING, betting or selling chances or to</td>
<td>...0003:0125</td>
<td></td>
</tr>
<tr>
<td>alcohol, hacking, remote proxies, or WAGERING, betting or selling chances or to</td>
<td>...0003:0125</td>
<td></td>
</tr>
<tr>
<td>use may include checking local news and WAGERING, betting or selling chances or to</td>
<td>...0003:0125</td>
<td></td>
</tr>
<tr>
<td>to audio, watching video (including JOB. Similarly, services such as</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>job. Similarly, services such as</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>unfortunately, external Hotmail, Yahoo, etc. Use of external</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>follows a three-tiered structure for Do</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>be submitted in digital format to 130.94.29.204 City</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>look and availability of the Town's 2) Make note of the</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>scanning programs check the Symantec WEBSITE for</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>and implementing appropriate &quot;</td>
<td>...0052:0018</td>
<td></td>
</tr>
<tr>
<td>unless there exists a legitimate WORK-AROUNDS &quot; during such time information systems</td>
<td>...0037:0045</td>
<td></td>
</tr>
<tr>
<td>research, development of WORK-ORIENTED need.</td>
<td>...0090:0151</td>
<td></td>
</tr>
<tr>
<td>and professional discussion in a WORK-RELATED deliverables and/or other work-related</td>
<td>...0005:0030</td>
<td></td>
</tr>
<tr>
<td>Communicating with other employees for WORK-RELATED field of knowledge</td>
<td>...0065:0025</td>
<td></td>
</tr>
<tr>
<td>A law enforcement officer or social WORK-RELATED purposes.</td>
<td>...0003:0078</td>
<td></td>
</tr>
<tr>
<td>long as it: (a) does not interfere with WORK-RELATED may need to originate or access traffic</td>
<td>...0069:0212</td>
<td></td>
</tr>
<tr>
<td>performance evaluation reports, WORKER productivity and (b) does not preempt</td>
<td>...0083:0070</td>
<td></td>
</tr>
<tr>
<td>as names of family, pets, friends, co WORKER compensation reports, and other related</td>
<td>...0080:0275</td>
<td></td>
</tr>
<tr>
<td>consultants, temporaries, and other WORKER'S, fantasy characters,</td>
<td>...0003:0261</td>
<td></td>
</tr>
<tr>
<td>WORKERS at Gaston County including all</td>
<td>...0002:0005</td>
<td></td>
</tr>
</tbody>
</table>
work schedule arrangement that allows WORKERS in accordance with departmental or are for the purpose of allowing entire WORKGROUPS or departments to share data. Requests
* Offer flexibility in the prevention of sexual harassment in the workplace, and to the principals of affirmative workplace and to refrain from using City...
prevent sexual harassment or hostile workplace violence, waste of corporate assets,...
Be sure to log out when you leave your workplace for more than a few minutes...
Be sure to log out when you leave your workplace for more than a few minutes...
anti-virus software and how to check a workplace or other device to determine if virus...
ingen all data written to or read from a workplace's hard drive. If it finds something...
SUBJECT:  WORKSTATION Use and Security...
4. The WORKSTATION - where the final scan for viruses...
all hardware (i.e., network devices, WORKSTATIONS, printers, scanners, mobile devices)...
screensavers shall be installed on all WORKSTATIONS. Such screensavers shall be set to...
all hardware (i.e., network devices, WORKSTATIONS, printers, scanners, mobile devices)...
hunting physical safeguards for all WORKSTATIONS that access e-PHI to restrict access to......
identifies physical safeguards for all WORKSTATIONS that access e-PHI to restrict access to......
Suite, Adobe, rich text files, HTML, the Firewall feature in Windows XP, such as but not limited to Hotmail, YAHOO, ...
Special backups will be retained for the project such as fiscal year or YEAR-END.
* Offer flexibility in the prevention of sexual harassment in the workplace, and to the principals of affirmative workplace policy in accordance with the Martin...