COUNTY OF WASHINGTON
COMMONWEALTH OF PENNSYLVANIA
100 WEST BEAU STREET
WASHINGTON, PA 15301

Information Confidentiality, Privacy, and Security Standards

Effective: June 1, 2003

Table of Contents

Overview

The purpose of the Washington County Employee Information Confidentiality, Privacy, and Security Standards Document is to set standards for the use of the Computer resources of the County. This policy driven standard is designed to help protect Washington County and its employees (employees, users, or computer users) from liability and business interruptions due to inappropriate use of County computers / telephones / software and breaches of computer security. It applies in conjunction with all applicable security and privacy regulations established by the Commonwealth and Federal government, such as HIPAA, to protect information transmitted by or stored in computer equipment.

This document sets forth what is, and is not, appropriate use of County computers and the employee's responsibility to safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. Employees may be disciplined for noncompliance with County policy.

This document is based upon the underlying policies adopted by the County and applies to each and every County employee, whether or not they are authorized computer users. It is the employee's responsibility to use sound judgment in the use of the Information Technology resources of the County and while this policy provides the basic policies of the County it cannot address every computer and security related issue. Should a question arise regarding the use of computers or issues related to the security of information that is not specifically addressed in this document the questions should be brought to the attention of your manager in a timely manner.

The Employee Information Confidentiality, Privacy, and Security Standards Document is subordinate to any collective bargaining agreement, employment contract, or other employment agreements.

Washington County may add to, or change, the policies and or standards at any time. Please read this document carefully and sign the Receipt of Employee Information Confidentiality, Privacy, and Security Standards Document form attached. The signed form will be placed in the employee's personnel file in the Human Resources Department.

Employees, Elected Officials, Department Heads, contractors an other individuals working in the County may from time to time use non-County owned computers and computer like devices in our environment. Before any such non-County device is connected to the County network, either by cable or via wireless technology, it must be inspected by one of the Information Technology staff to ensure that it has the minimum security, protection and connection abilities that are specified by this Standards document. Only after such inspection will a non-County owned device be allowed to access to the County network. Such connections are at the discretion of the Director of Information Technology and subject to periodic review. Once connected to the County network all security policies regarding information security and general computer use apply to the use of the non-County computer until the device is removed from the network, with the exception that documents need not be backed up and e-mail may be of a personal nature to the extent that the files and e-mails are confined to the non-County device.

Washington County
Information Technology Department
January 2003

Introduction

The County Department of Information Technology is so named because almost every employee has a computer, and most of the information that we use in our work environment is stored transmitted or handled with computer technology. It is vital that this information be safeguarded and our ability to use the information is protected from accidental or malicious losses. County management through this document is attempting to provide basic guidance on proper use of County computers and the safeguarding of County information as approved in the related County Policies.

Washington County is very supportive in the appropriate use current computer technology, including e-mail and the Intranet / Internet, to address the business needs of all County Departments. We do however have great concern for the potential misuse of this technology.

The County expects its employees, as public servants, to subscribe to normal and acceptable professional ethics when using these information technologies.

In an effort to establish and enforce reasonable and effective Standards for Employee Information Confidentiality, Privacy, and Security the following information is based upon official Washington County policy. It is designed to:

- Help prevent the violation of personal privacy rights
- Define and help prevent illegal activities regarding Information Technology
- Reduce the risk of liability and business interruption
- Maintain a professional work environment where computer abuse will not be tolerated
- Provide operational guidance in adhering to County Policy.

We believe this document provides the basic framework for addressing these issues and accomplishes in a reasonable and equitable manner the setting of standards that supports the various County missions to serve our citizens in a professional and cost effective manner.

Computer Users

The term "Computer User" includes County employees, consultants, and other County authorized persons. All Computer Users are responsible for the appropriate use of County computers, and for taking reasonable precautions to secure the information and equipment entrusted to them. County authorized computer users are responsible for reporting inappropriate use of County computers, and breaches of computer security, and assisting in resolving such matters.

Computer Users are responsible for adhering to County policies and practices as described herein, and in other County policy manuals, to ensure County computers are used in accordance with County policy guidelines, and reasonable measures are taken to prevent loss or damage of computer information and equipment.

Elected Officials, Department Managers

It is the responsibility of Elected Officials, Department Managers to assure that this policy is adhered to by all those under their supervision whether those they supervise are computer users or not. Elected Officials/Department Managers must report new hires, terminations, personnel moves, name changes, and **any type of unexpected absence of more than one consecutive week** to the Information Technology Department immediately. This is to be done in a formal written method using form "Schedule A" attached.

Confidentiality

General

All computer information is considered confidential unless you have received permission to share it.

Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use is prohibited. Accessing or attempting to access confidential data is strictly prohibited unless you are an authorized user of the information.

Handling Confidential Information

The following are considered inappropriate under normal circumstances when dealing with confidential information:

- Printing to a printer in an unsecured area where documents may be read by others
- Leaving your computer unattended with confidential files open on to your computer
- Leaving computer disks with confidential data unattended, in easy to access places. Remember it only takes a minute to copy a disk
- Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from departmental management and Information Technology management

If you observe a document at a shared printer, or any other location, do not read it without permission.

Encryption

Encryption of documents and files and the use of encryption utilities are prohibited without Information Technology management approval. If you need to send confidentiai or proprietary information over the Internet, or other public communication lines, you must obtain prior approval from management. The Information Technology depart will work with your department to provide the proper tools for the encryption of information and files. Some of the concerns that must be addressed include:

- Ensure that the Departmental Manager authorizes the use of data encryption for the specific data and purpose.
- Ensure the selection of the appropriate encryption and decryption techniques for the purpose
- Ensure that data that is encrypted can be decrypted by those required to do so
- Ensure that the level of encryption is sufficient for the intended purpose
- Ensure that the appropriate Department management has access to encryption and decryption keys

Unauthorized Access

- **Unauthorized access of County computers is prohibited.**
- **Unauthorized access of third-party computers, using County computers, is prohibited.**
- **Attempting to access County computers without specific authorization is prohibited.**

Any form of tampering, including snooping and hacking, to gain access to computers is a violation of County policy, and carries serious consequences.

Employees are required to turn their computer off at the end of the day, and when not in use for an extended period of time. This will help prevent computer security breaches, and damage due to power surges. In addition, employees must take other reasonable precautions to prevent unauthorized access of County computers.

Passwords

A Password is your signature. You would not sign a blank check and give it to a stranger, nor should you give your password to a stranger. You are responsible for actions taken under your user account and the key to your user account is your password. The County systems monitor the user account associated with activities. **Protect your password.** Do not leave it on a "sticky" pasted to your computer monitor, do not write it down on your calendar, and do not leave it where someone can see it.

Not only the County is at risk when someone gets your password. Computers often contain confidential information. If this information is accessed and distributed, it could cause great harm to you or someone you work with. Once someone gets your password, they have the capacity to use **your user account** to:

- Send e-mail to individuals, or groups, representing themselves as you
- Disseminate your files over the Internet
- Modify your computer our cause damage to programs
- Delete or alter files
- Share your password with other interested parties
- Monitor your work

Selection and Protection

Users will be held accountable for password selection and protection.

Select difficult passwords and change them regularly.

Do not share your password with anyone. Do not write it down where someone can find it, do not send it over the Internet, Intranet, e-mail, dial-up modem, or any other communication line. **Selecting the option "remember my password each time" is not permitted.**

Poor password selection and safekeeping is not an acceptable excuse if a hacker damages County computer systems using your password.

The following is a good guideline for password selection:

- Use 8 or more characters, both alphanumeric and numeric characters must be used
- Your password should not include your login name, your name, your spouse's or partner's name, children's or pet's name, or any other names commonly known to others
- Your password should not be a word pertaining to the County, your work, or an activity that you participate in or follow that is commonly known
- Your password should not include anything derogatory, offensive, or defamatory
- An example of an acceptable password is "thisdogwillnothunt345" or"89ilike2Work"

If you have a question about password selection or safekeeping, please see your supervisor or call the Information Technology Helpdesk.

Using Another Persons Password

Using a password assigned to another person is not permitted. The use of a password that is not assigned to you is a serious violation of County policy.

The use of another employee's password or access code to "log on" to that person's information service account is grounds for disciplinary action.

Password Access to Programs or Computer Hardware

Do not leave your computer logged on and unattended for an extended period of time. Exit applications before you step away from your work area. Do not log on to your system if someone can see you keying in your password. Turn off your computer when you leave at night. Furthermore, use a Windows or County supplied screen saver with password access to secure the computer from unauthorized access. A maximum time for the activation of the screen saver should be no more than 30 minutes, unless unusual circumstances indicate a longer time and the Department head authorizes the extended period.

Unauthorized Access

Prying, or attempting to explore areas where you are not authorized in the County's computer systems is a serious violation of County policy. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to management.

Watching other users enter information, and looking at computer disks that do not belong to you, are prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way, are violations of County policy. If you observe someone snooping or prying, report it to management.

Hackers

Hackers frequently penetrate computer systems by calling unsuspecting employees representing themselves as a new employee, executive of the County, or another trusted individual. Through a variety of probing questions, they obtain the information necessary for their hacker programs to do their work.

Never give any information about computer systems out over the telephone, or in any other way. If someone requests such information, get their name and phone number, and tell them you will get right back to them. Report the incident immediately to management. Without your help, the County has little chance of protecting its computer systems.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using County computers is prohibited, and will be reported to the local authorities. If you identify vulnerability in the County's computer security system, report it to management.

Viruses

It is critical that users make certain that data and software installed on County computers are free of viruses. The County provides virus-scanning software for your workstation and scans e-mail as it arrives at the County's mail server. This system or any system is not 100% effective. It is possible that you may encounter a virus before the anti-virus software has detection and fix information ready. Common sense in handling data and e-mails is our first line of defense; please help prevent serious problems. If you are unsure of a file or e-mail call the Information Technology Helpdesk for help.

Use of virus, worm, or Trojan horse programs is prohibited. If you identify a virus, worm, or Trojan horse, or what you suspect to be one, do not try to fix the problem. **Immediately turn your computer off, make notes as to what you observed, and contact the Information Technology Manager.** The principal concern is stopping the contamination before additional damage is done. These programs are most successful when ignored. They are designed to easily hop from application to application, contaminate a computer disk, and access another computer. The key to containment is limiting the reach of the contamination. Turning off your computer does this best.

Games

Washington County strictly prohibits the use of computer-based games on any County-owned computer.

Employees and Department Heads shall not purchase, allow to be installed, or use any computer games on County-owned computers.

Furthermore, if there are any "personal" (employee owned) computers being used within the County, computer-based games may not be used on them during working hours.

It will be the responsibility of each Department Head to make arrangements for the games that may currently exist on County computers to be removed. Once games are removed, it is the Department Head's responsibility to ensure that their personnel on the computers under their control do not install new games.

Information Technology will remove all games prior to installation of a new computer in the user's department. If, while doing routine maintenance, or responding to a help-desk call by the user, Information Technology Staff find games on a computer, they will make it known to the Department Head of the breach of policy. Once notified, and after the Department Head has addressed the violation with the offending employee, the Department Head shall make a request for Information Technology to remove the new game.

Physical Security

Computer Theft

The removal of County-owned computing or networking hardware or software from its assigned location is prohibited. Report any suspicion of theft to your department head immediately and to the Information Technology department. Theft is a crime and will be referred to the appropriate law enforcement persons when discovered.

Physical security is key to protecting your computer and computer information from loss and damage. Store floppy disks and other sensitive information in a locked drawer. Turn off your computer when it is not in use for an extended period of time. Lock the door to your office, if you have one. Take a few minutes to practice good physical security. Your investment of time will provide an excellent return, and help prevent temptation by others.

Laptops/Other Portable Equipment

The following are required when taking laptops or any other equipment off County property:

- Laptops/equipment must be signed out with the department manager in charge of that equipment. (Use Schedule B attached)
- Report lost or stolen computers immediately
- All important files must be backed-up, and back-up disks must be stored in a separate physical location from the computer
- Confidential, important, and proprietary data leaving the facility requires management authorization and all laptops must use the EFS (encrypting file system) encryption as specified in the internal IT departmental policy.
- Use reasonable precautions to safeguard the laptop against accidental damage
- When traveling, laptops must be in sight at all times or physically secure
- Always store laptops in a concealing carrying case.
- When not in use, store laptops/equipment in a locked drawer or trunk of vehicle.

The employee to whom the laptop/portable equipment is assigned is responsible to keep the equipment in good condition and to safeguard against theft at all times. Each case of loss or damage will be reviewed individually to assure that the employee adhered to established procedure and policy. If fault of the employee is determined, sanctions may be applied, including reimbursement to the County for the value of the lost or damaged equipment.

Off-Site Computers

Off-site users must take additional precautions to safeguard computer information and equipment, including but not limited to:

- Safeguarding the computer and information from theft or damage

- Prohibiting access to the computer (including family, friends, associates, and others) for any purpose, without management authorization
- Adhering to all computer policies and practices of the County for on-site users

Copyright Infringement

The County does not own computer software, but rather licenses the right to use software. Accordingly, County licensed software may only be reproduced by authorized County officials in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material is strictly prohibited.

Copyright laws apply on the Internet as well. There is no "but copying it was so easy" defense to copyright infringement. Copyright infringement is serious business, and the County strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with management immediately.

Copies of shareware or "free" programs must be registered and approved with the information technology department prior to download or installation. Shareware and free software often have licensing and use restrictions, and should not be copied or forwarded to others. Typically, if you continue to use shareware you must send in a "donation," often of a specified amount. If you neglect to do so, you may have committed copyright infringement. If you provide the program to a friend, you may have violated copyright law. It is not unusual for "free" software to contain a virus. As such, it is important that all new software that is to be installed on County equipment is registered with the Information Technology Department. Your supervisor and the Information Technology Manager must approve requests for application programs.

Harassment, Threats and Discrimination

It is Washington County policy, and the law, that employees are able to work free of unlawful harassment, threats, and discrimination. Unlawful harassment is physical, written, or verbal behavior directed towards an individual due to their race, age, marital status, gender, disability, religion, sexual orientation, or nationality for the purpose of interfering with an individual's work performance, or creating an intimidating or hostile work environment.

It is inappropriate and against County policy to use County computers to share your personal views about religion, politics, sexuality, or any other subject of a personal nature that could be considered offensive to others within or outside the County.

Deleted files are often easily recovered; and information on County computers is not necessarily private. Users often feel comfortable writing and storing files within the confines of their "personal" computer, and sharing personal views on a wide range of non-business subjects. Remember, whatever you transmit is a permanent record to the receiver. It can, at some future date, be taken out of context and used against you and the County.

Accidents, Mistakes and Spills

Take a few seconds to read the computer screen before you delete, save, or transmit files.

In addition, users need to take reasonable precautions with respect to computer operations, maintenance, handling, and transportation.

Placing liquids and other food items on your desk is strongly discouraged.

Unauthorized Changes to County Computers

Installing software and making changes to computer hardware, software, system configuration, and the like are prohibited, without management authorization.

Data used on home computers may become infected with a virus, and contaminate your computer and other County computers. **Do not bring disks or software from home for installation on a County computer and do not transport files between home and work computer via floppy disks.**

Purchases of Computer Software and Equipment

Purchases of computer software and equipment are prohibited without approval from departmental management and information technology management. All computer software and hardware purchases must be registered with the Information Technology Department, meet pre-established quality requirements, and be compatible with other County computer software and equipment.

All software will be installed by the Information Technology Department. This is to ensure that, not only is the software compatible with our systems, but that it does not contain a virus.

Disposal of County Data

Purge files, including outdated e-mails, which no longer have a practical use on a periodic basis (approximately every 90 days). Old computer files utilize disk space, and often represent a potential hazard to you and the County. Delete old personnel evaluations, compensation information, sales and financial information, customer information, and vendor data as specified by law or policy.

File Recovery

Computer files and e-mail are rarely erased from the system simply by hitting the delete key. Rather, they are stored in a random place on the computer. These files can be easily recovered by running a file recovery program. To actually erase a deleted file from existence, you must run a program to erase deleted files. Keep in mind that if the files are backed-up before you run the program, you again have an electronic record. Files stored on the LAN are much more difficult to erase. This is because the LAN is backed up automatically, and only the Information Technology Manager has access to run programs that will permanently erase a file from the server. The bottom line is, your deleted file is most likely permanently stored on back-up. For this reason, always conform to the highest, most professional standards when composing communications on the e-mail system and when doing any other task involving the computer.

Personal Use of Computers

Incidental and occasional personal use of County computers is permitted for reasonable activities that do not need substantial computer hard disk space, or other computer equipment.

Prohibited activities include, but are not limited to:

- computer games
- personal software and hardware
- running a personal business on the side
- Using County computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable, or political causes

If you are uncertain about a specific activity, ask your supervisor.

Proprietary Information

County data, databases, programs, and other proprietary information represent County assets and can only be used for authorized County business. Use of County assets for personal gain or benefit is prohibited. Sharing County proprietary information with unauthorized County personnel, or third parties, is prohibited.

Reporting Policy Violations

Employees are required to report violations, or suspected violations, of computer policy. Activities that should immediately be reported to management include, but are not limited to:

- Attempts to circumvent established computer security systems
- Obtaining, or trying to obtain, another user's password
- Using the computer to make harassing or defamatory comments, or to in any way create a hostile work environment
- Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others
- Illegal activity of any kind
- Using County computer equipment for personal financial gain at any time.
- Trying to damage the County, or an employee of the County, in any way

Computer policy violations will be investigated. Noncompliance with the County's employee computer policy may result in discipline up to, and including, termination. Employees that report violations or suspected violations of County policy will be protected from termination, discrimination, harassment, and any other form of retaliation.

If you identify computer security vulnerability, you are required to report it immediately.

Termination of Employment

All information on user computers is the property of Washington County. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination requires management authorization. The computer you have been entrusted with must be returned with your password, identification code, and any other appropriate information necessary for the County to continue using the computer, and information, uninterrupted.

Department Managers are required to submit the attached "Schedule A" to the Information Technology Department within 24 hours of an employee termination, whether the termination was voluntary or not. Terminated employees must complete and sign "Schedule C" attached and that schedule must be turned in to Human Resources for inclusion in their personnel file.

The following activity is prohibited upon termination, and will be prosecuted to the fullest extent of the law:

- Accessing County computers
- Providing third parties, or anyone else, access to County computers
- Taking or destroying computer files, data, programs, or computer equipment

Privacy and Monitoring

The contents of any information, in any format, stored by any means on the County's electronic facilities, including, but not limited to: (voice mail, "Email, Internet usage, computer network drives, hard disks, individual diskettes, or cd's or any other type of storage medium), is the property of Washington County and subject to inspection, at any time, without notice. Deleting of information from your files or storage medium does not mean that this information is erased and non-retrievable

Washington County reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications and information, and will do so for legitimate business purposes.

Random audits to verify that County computers are clear of viruses, and used in accordance with County policy, may be performed. Washington County will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. Washington County has software and systems in place that monitor and record all Internet usage. Our security systems are capable of recording (for each and every user) each World Wide Web site visit and the duration of time spent, each chat, newsgroup or e-mail message, and each file transfer into and out of our internal networks and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. County managers may review Internet activity and analyze usage patterns, and they may choose to publicize this data to assure that County Internet resources are devoted to maintaining the highest levels of productivity.

Again, computer systems and information are County property, and should be used principally for business purposes.

Lawsuits and Subpoenas

County computers, like any other County property, are subject to subpoenas. This means that prosecutors and plaintiffs' attorneys may access County computers, and look at information to gather evidence in a complaint.

It is not the County's intention to suggest that you remove any information from your computer, now or at any other time to in any way hinder an investigation of any kind. Quite the contrary, management prohibits such activity. Management's intention is to ensure that users conduct their work to the highest ethical standard with the knowledge that computer information (even deleted files) can be used against you and the County in a legal proceeding.

External Communications

Third Parties

The same standards of decorum, respect, and professionalism that guide us in the office environment, apply to computer communications with third parties. Important, confidential, and proprietary information is stored on County computer systems. Accordingly, only County personnel are allowed access to the County's computer systems, without written authorization from management. Management must approve computer data and other information received by, or provided to, third parties. Please keep in mind that third parties may have a legitimate business need, duty, legal right, or obligation to access, disclose, or use information transmitted.

Internet

Copyright laws can be enforced on the Internet. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. People who would like to harm the County or its officials and employees exist on the Internet. Hackers exist on the Internet. As such, users must follow established computer operating policies and practices to reduce the opportunity for security breaches, and inappropriate or illegal activity resulting from connecting to the Internet.

Internet Connections

Internet connections are authorized for official Washington County business needs only. Connection from County equipment or using County resources to connect to the Internet without management authorization is prohibited. Any unauthorized usage of the Internet facilities, resources or infraction of the County's policy will be cause for severe disciplinary action.

Furthermore, the following activities are prohibited:

- The County has installed an Internet firewall to protect the safety and security of the County's networks. Any employee who attempts to disable, defeat or circumvent this, or any other County security facility will be subject to immediate dismissal.
- Downloading information of any kind, including data, files, programs, pictures, screen savers, and attachments, unless such activity is a recognized function of the employee's job or is authorized by the Director of Information Technology.
- Using the Internet for fun, personal profit, political activities, or illegal or illicit activities. Use of the Internet for illegal or illicit activities shall be grounds for suspension or immediate dismissal.
- Establishing communications with third parties without management or department approval
- Forwarding or transmitting information to third parties or employees unless such transfer is a specific job function and approved by Information Technology and the Department manager
- Copying programs, files, and data
- Transmitting important, confidential, or proprietary information
- Speaking on behalf of the County unless authorized by the appropriate County Officials
- Accessing or attempting to access computer based records or services that an official or employee does not have specific authorization to utilize.

Individuals that have received management approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the County. Disclaimers such as "The opinions expressed do not necessarily represent those of the County," while a good idea, do not necessarily relieve the County of liability. The Internet should be considered a public forum for all transmissions. All communications on the Internet provide an opportunity for a permanent record, and can be edited and retransmitted. Accordingly, maintain a professional decorum in all communications and transmissions.

The following actions are prohibited under any circumstances:

- Portraying yourself as someone other than who you are, or the County you represent
- Accessing inappropriate web sites, data, pictures, jokes, files, and games
- Inappropriate chatting, e-mail, monitoring, or viewing
- Harassing, discriminating, or in any way making defamatory comments
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes
- Gambling or any other activity that is illegal, violates County policy, or is contrary to the County's interests

Washington County may use independently supplied software and data to identify inappropriate or sexually explicit Internet sites. The County can and will block access from within its networks to all such sites that the County knows of. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program, and report it at once to your immediate supervisor. The supervisor in turn must report the site to the Information Technology Helpdesk.

Employees may use their Internet facilities for non-business research or browsing during mealtime or other breaks, or outside of work hours, provided that all other usage policies are adhered to.

Remote Access

The County will provide based upon management approval the ability to access the County network and County e-mail from external computers based in part upon a technology referred to as VPN and must be established and verified by the Information Technology department. If there is a need to have access to the County network via the Internet please contact your department head. Department heads are required to authorize the remote access request before the Information Technology department will establish the remote access account.

The use of programs such as PC Anywhere is actively discouraged and the use of PC's with modems connected or installed are subject to prior approval by the respective Department head and IT.

Users are required to turn off dial-up modems at the end of the day. Modems must be programmed to pick-up after the fourth ring (this will help prevent unauthorized access). Users are required to turn off remote access programs within a reasonable time after use, usually 5 to 10 minutes. Downloading or uploading confidential or proprietary information requires approval by Departmental Management and Information Technology management.

Screen Savers/Wallpaper

Use of any screen savers/wallpapers other than those provided in the computers operating software is not permitted unless authorized by the Department of Information Technology.

E-mail

Electronic Communications

The Electronic Mail, (e-mail) system, provided by the County of Washington, is the property of Washington County and is provided for the purpose of conducting County business. Conducting personal business on the County e-mail system is prohibited. All messages composed, sent or received on the County e-mail system are and remain the property of Washington County. Every employee has an e-mail account provided by the

County, and use of any other "third party" e-mail accounts, such as hotmail accounts for **"official"** County communications is prohibited.

Communications by e-mail should be drafted with the same care as a formal memorandum and should not contain informal remarks that might potentially be embarrassing to the sender, the receiver, the employees of the County, its' Elected Officials or its' residents, or contain information that is not defensible in a court of law. The contents of e-mail should not include anything, which the sender would not want publicly disclosed.

Information, stored in an electronic medium, is potentially neither private nor inaccessible by others and may be subject to discovery in a legal proceeding. County e-mails are automatically stored on a computerized backup system. The County reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose. The contents of electronic mail properly obtained for legitimate business purposed, may be disclosed within the County without the permission of the employee.

Only County personnel are allowed access to the County e-mail system and only County business is to be conducted through this medium. The following e-mail activity is prohibited:

- Accessing, or trying to access, another user's e-mail account
- Obtaining, or distributing, another user's e-mail account
- Using e-mail to send harassing, discriminating, intimidating, offensive or defamatory comments. An offensive message is one which contains sexual implications, racial slurs, gender-specific comments, or one that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.
- Using e-mail to send off-color jokes, sexually explicit images, cartoons, jokes, or messages, vulgarities, obscenities, sarcasm or exaggerations.
- Transmitting County records within, or outside, the County without authorization
- Transmitting junk mail, chain letters, Spam, or soliciting for commercial, religious, charitable, or political causes or other non-job-related solicitations.
- Transmitting confidential or sensitive information relating to employees, clients or County Business.
- Transmitting personal communications

Employees are required to report inappropriate use of e-mail.

Forwarding Information

If you receive e-mail (particularly e-mail with an attachment) and intend to forward it to others, consider the following:

- Is any of the information unnecessary or inappropriate for any individual?

- Would the author take exception to, or be embarrassed by, your forwarding the information? (A good rule of thumb is to copy the author.)
- Might the information be received negatively?
- Might the information be misunderstood?
- Is the receiver likely to forward the information to individuals that should not have, or do not need, the information?
- Do the attachments have viruses?

If the answer to any of these questions is yes, do not forward the information. Edit it, or create a new file.

Spam

Sending unsolicited messages or files to individuals, groups or organizations that you do not have a prior relationship with is prohibited, without written authorization from your supervisor. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of County policy and will be prosecuted to the full extent of the law.

Local Area Network (LAN)

All important, confidential, or proprietary information must be stored on the Local Area Network (LAN). Storing information on your desktop computer is prohibited, without authorization from management. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and back up are performed on the LAN daily; and programs and other information are updated regularly.

All County policies apply to the LAN. The following activities are prohibited, without management authorization:

- Installation of business or personal software on the LAN
- Making any changes to the LAN hardware or software
- Accessing without authorization, or exceeding authorization, LAN programs, data, and files
- Assisting anyone within, or outside, the County in obtaining access to the LAN

If authorized by your Department Manager to store information on the local computer, you must back up important files daily. All backed –up files should be stored on a secure computer disk or tape, other than the one containing the original data. The back-up disk or tape should be stored on-site, preferably in a locked drawer or where possible off-site in a secure area.

Glossary of Terms

Computer Information
Data, software, files, and any other information stored on County computers and systems.

Encryption
The process of turning plain text into cipher text by applying an algorithm that rearranges or changes its input into something unrecognizable.

Firewall
A specifically configured system that serves as a secure gateway between an outside network (e.g., the Internet), and the organization's internal networks.

Hacker
Slang, an individual intensely absorbed with and/or extremely knowledgeable about computer hardware and software. Also used to describe those who break into and corrupt computer systems. (Hacker is used here to describe those who break into and corrupt computer systems.)

Intranet
A local area network which may not be connected to the Internet, but which has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so employees have access to the organization's Web documents.

Internet
The World Wide Web. A group of networks connected via routers.

ISDN
Integrated Services Digital Network. Digital telecommunications lines that can transmit both voice and digital network services, and are much faster than the highest speed modems.

LAN
A set of connections between computers that provides the basis for electrical transmissions of information, generally within a small geographical location to serve a single organization.

Login
A start-up file stored in the user's directory. This file is used to execute commands that should only be executed at login time, such as establishing the terminal type and starting windows systems.

Modem
Short for modulator-demodulator. A hardware device that allows two computers to communicate over ordinary telephone lines.

RAM
Random Access Memory. The working memory of the computer. RAM is the memory used for storing data temporarily while working on it, running applications programs, etc. "Random Access" refers to the fact that any area of RAM can be accessed directly and immediately.

Server
A computer or device that administers network functions and applications.

Trojan horse
A program that masquerades as something it is not, usually for the purpose of breaking into an account or exceeding commands with another user's privileges.

Virus
Sets of instructions that can reside in software; and can be used to destroy other files or perform other tasks with another user's privileges.

Web Site
A server computer that makes documents available on the World Wide Web. Each web site is identified by a host name.

Worm
A program that propagates by replicating itself on each host in a network, with the purpose of breaking into systems.

Receipt of Washington County Information Confidentiality, Privacy, and Security Standards Document

I have received and read the Washington County Information Confidentiality, Privacy, and Security Standards (revision 01/23/2003) I am responsible for adhering to the policies and practices described therein. I understand that these policies may be added to, or changed by Washington County at any time. It is my responsibility to bring any questions I have about the Information Confidentiality, Privacy, and Security Standards to my supervisor. I further understand that it is my responsibility to report any violations of this policy that I witness, or become aware of, during the course of my employment.

As an employee of Washington County, I understand that the County's e-mail; internet/intranet, telephone and voice mail systems are County property and are to be used for conducting County business only. I understand that use of this systems/equipment for private purposes is prohibited.

I am aware that the County reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the County's e-mail, internet/intranet, telephone and voice mail systems at any time, with or without employee notice, and that such access may occur during or after working hours. I am aware that use of a County-provided password or code does not restrict the County's right to access electronic/voice communications. I am aware that violation of the Washington County Information Confidentiality, Privacy, and Security Standards may subject me to disciplinary action, up to and including discharge from employment.

_____________________________ _______________

Employee Signature Date

____

Employee Name (Please Print)

_____________________________ _______________

Witness by Department Manager Date

Schedule C

Employee Termination Computer Checklist

(To be completed by Employee)

□ Have you returned to the County any and all equipment entrusted to your care, including, but not limited to laptop, desktop, pager, cell phones, printers, scanners? ___________

□ Have you returned disks, tapes or CD ROMs with important, proprietary, confidential or sensitive information on them? _______________

□ If the answer to II above is yes, to whom have you returned them?

____

□ Do you currently have access to County computers? __________ If so, which ones? ____________________________________

□ Has your user identification code and password been canceled? ___________

□ Did you delete or substantially alter any computer data, files or programs upon your termination? __________________________

□ Have you retrieved your voice mails and canceled your voice mail password?____________

□ Is there any reason that the County cannot access, or will have difficulty accessing, computer information previously controlled by you? ________

□ I certify that the foregoing has been answered truthfully. I agree that, since I no longer have am under the employ of Washington County that I will not try to gain access to any of the County's computer systems or provide information to help others gain access to County computer systems.

Signature of Employee: __________________________ Date: __________________

Schedule B

Computer Property Sign out

I (Print Name) ________________________________ have received the following equipment on this date. I agree to maintain it in good condition, immediately reporting damage or loss to my supervisor. I agree to return this equipment to the County at the end of its useful life or upon my termination of employment with Washington County whichever comes first.

Equipment Type	Manufacturer	Serial #	Fixed Asset #	Cell/Pager #
Laptop				
Cell Phone				
Pager				
Other				

Signature of Employee ________________________________

Date: ______________________

Schedule A

Information Confidentiality, Privacy, and Security Standards

Notice of Staff Status Change

To: Director of Information Technology
From: ____

The following change in status is effective (date) ________________________
Staff information

Name: ____

Position: ____

Reason for Status Change:

- □ New Hire
- □ Job Duty Change
- □ Retired
- □ Terminated
- □ Absent for more than 1 week without Notice
- □ Other ____

Actions Requested:

- □ User Name and Password [ ] Assigned [ ] Canceled
- □ Access to the following special program(s)

  ____

  ____
- □ Internet Access [ ] Granted [ ] Revoked
- □ Suspension of Account Access
- □ Other as Specified

  ____

  ____

Requestor: _______________________________________ Date: ________________

IT Acknowledge: _________ Date: _________
IT Completed: ___________ Date: _________

ADOPTED this 19th day of June, 2003, per minute # 722 .

ATTEST:

Catherine E Kresh

Catherine E. Kresh, Chief Clerk/
Administrator

COUNTY OF WASHINGTON

John P. Bevec, Chairman

Diana Irey

Diana L. Irey, Commissioner

J. Bracken Burns, Sr., Commissioner

APPROVED AS TO FORM AND LEGALITY:

Richard DiSalle
County Solicitor

Michelle Miller Kotula

Michelle R. Miller-Kotula
Human Resources Director

Dan Briner
Director of Information Technology