INFORMATION TECHNOLOGY SECURITY POLICY

Summary: *To be effective, Information Technology Security must involve the participation and support of every Pierce County worker who accesses Electronic Public Records and Computer Systems. This policy statement identifies the responsibilities of the End User, as well as the steps they must take to ensure the appropriate protection of Pierce County electronic records and functions.*

DEFINITION OF TERMS

Authentication: The process of verifying the identity of an End User or computer process.

Computer System: The set of computer hardware and software components used to provide or support a Pierce County function, and/or to hold Electronic Public Records. Computer Systems include stationary and mobile computers assigned to workers.

Computer Infrastructure: The data centers, networks, hardware, and software that support Computer Systems.

Electronic Public Record: A Pierce County public record, as defined by RCW 42.56.010, that was retained on a County system through electronic means. The record may be exempt from public disclosure.

End User: An End User is any person, including those who are affiliated with a third party, who uses any Computer System that is not publicly-available or requires authentication.

Information Technology Security: The practice of protecting Electronic Public Records, Computer Systems, and Computer Infrastructure.

POLICY

In order to protect Pierce County Electronic Public Records, Computer Systems, and Computer Infrastructure, all End Users are required to adhere to Pierce County's Information Technology Security Standards in Attachment A; all applicable state or federal rules governing Pierce County data, such as the Revised Code of Washington (RCW); the Health Insurance Portability and Accountability Act (HIPAA); the Criminal Justice Information Services Security Policy (CJIS); and the Payment Card Industry Security Standards (PCI).

STANDARD

This policy applies to all End Users. End Users are responsible for familiarizing themselves with, and complying with all Pierce County policies, procedures, and standards dealing with Information Technology Security.

PROCEDURE

Non-compliance subject to disciplinary action: Non-compliance with information security policies, standards, or procedures is grounds for disciplinary action up to and including termination.

Required reporting of violations and suspicious activity: All End Users have a duty to report to their department management and the County Information Technology Security Officer on a timely basis all information security violations and problems so that prompt remedial action may be taken.

Effective:	*February 1, 2019*
Last Revised:	*August 2015*
	August 2014
	March 2007

References: Pierce County Charter, Article 9, Section 9.60 – Information Management; Pierce County Code, Title 2 – Administration, Section 2.06.010 J. Information Technology

ATTACHMENT A
INFORMATION TECHNOLOGY SECURITY STANDARDS

The Finance Department Director has delegated IT security oversight responsibility to an Information Technology Security Team. The Information Technology Security Team will provide direction on IT security issues, and will develop, monitor, and review IT Security Standards.

Definition of Terms

Alias Account: A logon account that is created for computer system work by a person that requires an additional account due to the need for testing, temporarily elevating privileges, or other situations that cannot be conducted or accommodated with a Primary Account.

Browse: Casual viewing.

Computer System: The set of computer hardware and software components used to provide or support a Pierce County function, and/or to hold Electronic Public Records.

Critical information: Any information essential to Pierce County's activities, the destruction, modification, or unavailability of which would cause serious disruption to the mission of Pierce County.

Data Custodian: Data Custodians are in physical or logical possession of either Pierce County information or information that has been entrusted to Pierce County. While Information Technology staff members clearly are Data Custodians, administrators of shared Computer Systems are also Data Custodians. Whenever information is maintained only on a personal computer, the user is the Data Custodian. Data Custodians are responsible for safeguarding the information, including implementing access controls to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost.

Data Steward: The department managers or their delegates within Pierce County who bear responsibility of the acquisition, development, and maintenance of databases which house Pierce County information.

Decryption: The mathematical process by which an encrypted message is rendered readable or usable (reverses the encryption process), also called decipherment.

Default Password: Refers to a password provided by a vendor with a software package.

Electronic Public Record: A Pierce County public record, as defined by RCW 42.56.010, that was captured through electronic means. The record may be exempt from public disclosure.

End User: An End User is any person, including those who are affiliated with a third party, who uses any Computer System that is not publicly-available or requires authentication.

Encryption: Encoding messages or information in such a way that it can only be read by authorized parties.

Initial Password: Refers to the temporary password provided to an End User when they are granted access to a Computer System, or when their previous password has expired.

IT: Information Technology Division of the Finance Department.

IT Security Team: A team of IT staff, comprised of the Assistant Director of IT, IT Security Officer, all IT managers, and expert systems engineers from every major discipline area, who provide governance functions that support Pierce County's cybersecurity responsibilities.

On-Premises Network: The set of stationary computers, managed by Pierce County IT, at a physical location where access is restricted to Pierce County workers and where the computers are not directly publicly-accessible,

Password: Any secret combination of letters and numbers used to identify an End User or computer process.

Personal Information Number (PIN): Any secret combination of numbers used to identify an End User.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, license plate number, credit card number or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII is protected information unless it is lawfully made available to the public from federal, state, or local government records.

Primary Account: The unique login name assigned to every End User for access to County Systems to conduct typical user functions such as email, word processing, time entry, leave requests, financial approvals, etc.

Protected Information: Information that is exempt from public disclosure per the Public Records Act (RCW 42.56), Attorney-Client Privilege Statute (RCW 5.60.060 (2)(a)), Washington State Court Rules, Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Criminal Justice Information Services (CJIS) Security Policy, and all other applicable state and federal laws. The Public Records Act exempts certain personally identifiable information (PII); investigative, law enforcement, and crime victim information; employment and licensing information; real estate transactions; financial, commercial, and proprietary information; preliminary drafts, notes, recommendations, and intra-agency memorandums; and attorney work product (records not available to another party under the Superior Courts' rules of pretrial discovery).

Screen Lock: A function that will automatically hide the screen contents of a computer monitor either through user initiation, or after a certain period of no activity.

Service Account: An account that is used by an application or process and may be shared by the service administrators. The account name should identify the initiating application or process. A service account is commonly used for a system backup, system data transfer, or shared kiosk.

Shared Account: An account with a role-based title where login credentials are shared by multiple individuals.

Shared Password: A password known by and/or used by more than one individual.

Strong Authentication: "Techniques that permit entities to provide evidence that they know a particular secret without revealing the secret." In more practical terms, it is a system of verifying the identify of an End User or computer process in which the parties must demonstrate knowledge of a "secret" rather than transmit a password. Typically, the verification is done via a trusted third-party authentication device (key fob) or service using conventional cryptography.

User Device: An interactive computing device such as a desktop, laptop, workstation, tablet, or smartphone.

User-IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Anti-Malware Screening Software: Commercially available software that searches for certain bit patterns or other evidence of computer virus infection.

Standards

SYSTEM ACCESS CONTROL

Accounts/User-IDs: Logon account type determination for each specific purpose must match the corresponding definition from the 'Definition of Terms' section in this policy.

Additionally:

- Primary Accounts must be associated with a single assigned End User who is responsible for all activity associated with the account. Primary Accounts are typically how a user logs into a computer to conduct normal work functions in the completion of their assigned duties.
- An Alias Account must be associated with a single assigned End User who is responsible for all activity associated with the account. Alias Accounts are typically used where someone needs to log into a system with different privileges than their Primary Account.
- Service Accounts must not be used for interactive user logon activities of any kind. Service Accounts have stronger password standard requirements. Appropriate uses of Service Accounts include embedding credentials required for scheduled automated tasks, such as periodic data backups and integrations with other systems. Service Administrator Teams using Service Accounts should safeguard credentials and be accountable for the account's actions.

- Shared Accounts should only be requested when it is not feasible to use a Primary, Alias, or Service account. Shared Accounts must obtain IT Security Team approval before they can be created. Password sharing for Shared Accounts should be extremely limited and passwords must be changed on a regular basis, no less than every six months or after public use.

Password Standards: Passwords must comply with the "Information Technology Password Standards" as set forth in the policy of the same name. These standards will be applied to the settings used by the password management software.

No Sharing of Passwords: Passwords must not be shared or revealed to anyone else besides the authorized End Users. To do so exposes the authorized user to the responsibility for actions that the other party takes with the password.

In an effort to be more productive or to save time, users have shared their passwords. Unauthorized use of systems is often done using someone else's username. Sharing passwords with others exposes the user and Pierce County to a security threat. Sometimes system attackers masquerade as though they are IT staff, and then ask users for their passwords. When requested to do so, a surprisingly large number of users will readily provide their password. Whenever users disclose their passwords, they inadvertently compromise system access controls and make log records less useful. It is important that users keep their passwords exclusively to themselves.

Inactivity Screen Lock Requirement: All County user devices will be configured to automatically apply a screen lock after 15 minutes (or less) of inactivity and require the End User to enter their password or PIN to continue use of the device.

Departments may request exemptions for specific computers due to negative impact on a critical business function or life safety situations. Exemptions must be approved by Information Technology Security Team, Finance Director, and Department Head. This standard prevents Protected Information contained on Pierce County devices from falling into the hands of unauthorized persons.

Securing Mobile Devices: Mobile County devices include laptops, tablets, and smart phones that are not securely mounted at a County facility or in a County vehicle. A mobile device is required to use full disk (storage) encryption. The addition of pre-boot authentication will be required if the device contains Protected Information.

This standard prevents Protected Information contained on Pierce County mobile devices, used regularly outside of County offices, from falling into the hands of unauthorized persons. Apple iPads and iPhones meet the requirements for full storage encryption and pre-boot authentication if the device is protected by a passcode. Windows laptops and tablets require additional software/configuration.

Use of Strong Authentication: All End Users outside Pierce County's on-premises network wishing to access a Computer System must authenticate using an approved strong process (two factor),

unless a specific exemption has been granted by the Information Technology Security Officer. Designated public systems, such as internet websites, do not need these authentication processes because anonymous interactions are expected.

Strong authentication (two factor) is a more secure and more verifiable way to manage individual personal access to systems and data and replaces the traditional username/password. This authentication is done by replacing a single known secret, with the combination of at least two of the following:

- What a person knows as a secret, such as a password or a Personal Identify Number (PIN)
- What a person uniquely has, such as an assigned phone
- What a person individually is, such as a fingerprint, face geometry, or other biometric data

This standard ensures that access to Pierce County Computer Systems is allowed only to known authorized users. User authentication systems prevent intruders from guessing fixed passwords, or from using passwords captured via a wiretap.

Mobile computers such as laptops, tablets and smartphones that are managed by Pierce County IT are configured with a form of two-factor authentication so that the computer can be considered something the person uniquely has.

Must Change Default and Initial Passwords: All default and initial passwords must be changed before any computer or communications system is used for Pierce County business. Default (widely known) and initial passwords are known by more than the user, so they are susceptible to misuse. By changing the default or initial password, it ensures that only the user knows the password.

Privilege Management: Accounts will be granted only those privileges/access rights necessary to complete their job duties. Service Accounts will only be granted those privileges/access rights necessary to complete their assigned purpose.

Local admin rights on computers are used successfully by malware writers to gain access to protected data and create havoc. By limiting user rights to just what users need to complete job duties, it eliminates many vulnerabilities that would otherwise exist if users are given full rights to systems they use.

User End of Service User-ID Controls: All User-IDs (except approved shared, purposed accounts, or group User-IDs) assigned to a departing user must be removed from all Pierce County Information Technology applications, servers, equipment, and services within 10 working days of end of service as an authorized user of Pierce County systems.

Shared, purposed account, or group User-ID(s) assigned to a departing user must be reassigned to another active user. The re-assignment must be approved by the responsible Data Steward and reported to the Information Technology Division System Administration Group (ITSystemAdmin) for

processing. Passwords or authentication procedures to these User-IDs must be changed (according to reassignment procedures established for each User-ID) within 10 working days of reassignment.

Procedures will be followed so that removal or reassignment of a User-ID will not cause loss of electronic records without authorization from the Data Steward.

It is tempting to keep a User-ID around "just in case" access is needed after the user leaves. This leaves our systems open to potential break in by the departing user or another unauthorized user since the account is no longer monitored by an active user. In the cases of electronic mail records or file server home directory, with proper approval, department heads can request the contents of a departed user's email be archived for safekeeping. The User-ID will be deleted after the data is appropriately stored and within 10 working days of the user's departure.

No Auto Embedded Login: All users must be positively identified prior to being able to use any multi-user computer or communications system resources. Use of auto embedded login shortcuts is prohibited, except where authorized by the IT Security Team.

The use of an auto embedded login sidesteps the identification process for logging into a system by "hard coding" the user's password in a script. The user's password is saved in the script for anyone with access to the script to use. This standard ensures that no unauthorized persons access Pierce County computers, or communication systems. Each time a user logs into a new system, a password that is unique to the individual needs to be entered by the user.

Security Warning Banner: Computer system owners/operators should display security warning banners prior to allowing logon to be initiated by users. These banners should inform users that the system or operation being accessed is proprietary and should only be used by authorized users.

A Security Warning Banner is the electronic equivalent of a no trespassing sign. For legal reasons, it notifies all that the involved system is for authorized purposes. An example banner is as follows:

This system is intended to be used solely by authorized users for legitimate Pierce County business. Users are monitored to the extent necessary to properly administer the system and to investigate unauthorized access or use.

NETWORK

Changes to Network Not Allowed: Users will not make extensions, modifications, or replacements to the network. Changes to the network can and often do inadvertently introduce vulnerabilities. This standard allows Information Technology, and other individuals authorized by Information Technology, to control modifications to the Local Area Network (LAN).

All Connections Must Be Authorized: Users are prohibited from connecting auto answer enabled dial-up modems, wireless access points, or cable modems to workstations which are simultaneously connected to a Pierce County LAN or another internal communication network.

This standard prohibits users from establishing a weak link in a system of network access controls. If a workstation is connected to the Pierce County network and connected to an external network via a PC modem, the connection can allow unauthorized parties on to the internal network (sometimes without a password or any other access controls). These types of connections may allow unauthorized parties to access LAN servers, and other systems connected to the internal network.

MALICIOUS SOFTWARE

County computers must be configured to protect against malicious software. Pierce County users are to consistently use malware protection software per the "Business Computer Equipment Use Policy." Additionally, Pierce County users will utilize the County's centralized patch management service to keep their operating system software up-to-date and secure. This standard ensures that all computers run protection software against known security risks from viruses, worms, etc., as well as to safeguard them from potential risky behavior by software trying to infect a computer.

Intrusion Protection Software: Pierce County computers should run and comply with the County's standard firewall/intrusion protection software to protect the devices from malicious software. The intention of this standard is to protect County computers and the County network from malware attacks that can enter our network and begin infecting devices before signature-based protection (anti-malware) is available and put in place to protect from a new threat.

Periodic Connectivity of Mobile Computers for Security Updates: All mobile computers should connect to the Pierce County network at least once a month to receive updated security software. Mobile computers must periodically connect to the Pierce County network to obtain the latest operating system software updates, anti-malware signatures, and intrusion prevention rules. If once per month is not practical, the devices should connect and obtain updates prior to being used on any external network. This practice is necessary in order to prevent contamination of the County's network when the remote device is reconnected to the County network.

DATA SECURITY

Those With Custody of Sensitive Information Must Restrict Access: Workers in custody of Pierce County sensitive information must take appropriate steps to ensure that these materials are not available to unauthorized persons. Employees or contractors who have custody of sensitive materials have a duty to restrict access to these materials. The policy is deliberately general about the ways to restrict access since these will vary by situation. Note that being in custody of sensitive materials is different than being a Data Custodian.

Storage Media Must Be Cleansed Before Disposal: The disposal of any storage media, or computer hardware which includes storage media, must include the removal and cleansing of County data from the storage media. Storage media includes, but is not limited to tapes, cassette backup tapes, CDs, disks, disk drives, copier hard drives, flash drives, and USB sticks. This standard prevents the

inadvertent release of sensitive County data. Since "deleted" data can be read, the cleansing process should be such that it renders the data unrecoverable.

Only IT Approved and Supported Encryption Methods Will Be Used: Encryption tools and processes used for Pierce County information must be adopted, supported, and managed by Pierce County Information Technology. This standard prevents users from damaging or destroying Pierce County information because they don't have the expertise or knowledge required to use encryption tools properly. The Information Technology Security Team approves all encryption tools to ensure adequate safety nets exist to recover the impacted information.

Protected Information: Protected Information is information that is exempt from public disclosure per the Public Records Act (RCW 42.56), Attorney-Client Privilege Statute (RCW 5.60.060 (2)(a)), Washington State Court Rules, Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Criminal Justice Information Services (CJIS) Security Policy, and all other applicable state and federal laws. The Public Records Act exempts from disclosure certain personal information (PII such as credit card numbers, bank or other financial information, and social security numbers); investigative, law enforcement, and crime victim information; employment and licensing information; real estate transactions; financial, commercial, and proprietary information; preliminary drafts, notes, recommendations, and intra-agency memorandums; and attorney work product (records not available to another party under the Superior Courts' rules of pretrial discovery). The intention of this standard is to provide a list of known protected information that may be accessed by Pierce County users.

Storing Sensitive Information on Mobile Devices: Workers in the possession of mobile devices such as a laptop, tablet, or smart phone containing sensitive Pierce County information must not leave these devices unattended at any time unless the information has been protected. Mobile devices are required to have a password to access, or use, the device with a timeout password of no more than 15 minutes.

This standard prevents sensitive information from falling into the hands of unauthorized persons. Protection can include encryption, a secured enclosure, or password protection on files.

Removal of Sensitive Information from Pierce County Premises: Sensitive Pierce County information may not be removed from Pierce County premises unless there has been prior approval from the Data Custodian. This includes but is not limited laptops and to mobile devices, CDs, hard copy output, and other storage media. An exception is made for authorized offsite back-ups, and laptops and mobile devices with encrypted data storage. The intention of this standard is to prevent sensitive information from traveling around, and in the process being potentially disclosed in unauthorized ways.

Browsing on Pierce County Systems and Networks Prohibited: Workers must not browse through Pierce County computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job is not considered browsing.

This standard prohibits hacking, cracking, and related activities. In many instances, perpetrators of computer abuse are exploring, rather than being deliberately malicious. However, these people may go on to take advantage of the information they discover (such as credit card numbers). When

caught, these people often claim that they were only looking around, and that they had no malicious, fraudulent, or other bad intentions. To counteract such claims, this policy states that non-work-related browsing of information systems is not acceptable.

IT Security Awareness Training: Pierce County users should complete IT Security Awareness Training on a regular basis using the resources made available by Information Technology. This standard encourages security training for all County employees to help protect County systems and data.

PHYSICAL SECURITY

Physical Access Is Limited: Access to the County's internal network and telecommunications infrastructure, software applications, and computers must be limited to County employees and other authorized individuals. The IT Security Team and/or other staff as delegated will therefore take steps to identify and analyze potential security threats and devise appropriate mitigation strategies, protocols, or procedures to ensure that facilities, network and telecommunications infrastructure, and computer-related assets are not exposed to unauthorized access or threats. Specific standards are as follows:

- Data centers will be secured with card reader and PIN. IT equipment rooms will be secured with card reader and PIN if access control is in use in the building. Otherwise, these locations will be secured with a cipher lock.
- Unattended computers, or live data jacks on the Pierce County network, are not allowed in places where the public can access without an escort, monitor, or locking mechanism on the data jack.
- Public use computers must be authorized through IT security review and lock down procedures.

The Office of the Washington State Auditor guidelines (State Auditor Bulletin # 3 GC-11) require that the physical access of computer hardware be limited to authorized individuals. All Pierce County users must comply with these standards.

Physical Control of Information Technology Assets: Information Technology assets must be tracked in Information Technology's computer asset inventory system for inventory control, accounting, and asset management purposes using standard identification and asset management tags. A reliable database of Information Technology assets enables Pierce County to define, locate, control, and better manage assets. Equipment inventories are also used in establishing regular equipment upgrade schedules.

PROHIBITED ACTIVITIES

- Any unauthorized deliberate action that damages or disrupts computing systems, network, or data, alters their normal performance, or causes them to malfunction or be unavailable, regardless of location or duration.
- The unauthorized use of remote control software for controlling hardware, software, or data.
- The willful or negligent introduction of computer viruses, or destructive programs, into Pierce County systems or networks, or into external systems and networks.
- The unauthorized decryption, or attempt to decrypt, any system, user password, or any other user's encrypted files.

- The use of packet-sniffing, packet-spoofing, or any other means to gain unauthorized access to a computing system or network.
- The use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
- Any conduct that would constitute, or encourage a criminal offense, give rise to civil liability, or otherwise violate any local, state, national, or international law, including without limitation to US exports control laws and regulations.
- Any disclosure of confidential or proprietary information to unauthorized individuals.
- The transmission of unsolicited or unauthorized, private, commercial, advertising, or political material to any individual, groups of individuals, or organizations and includes but is not limited to, transmissions that deliberately overload systems, or network equipment (a.k.a. "spamming" or "denial of service").
- The use of unauthorized tools to compromise security.
- Disabling security protection software, or installing, or using software which poses a security risk.

CONTINGENCY PLANNING

Users must verify that their sensitive, critical, and valuable data is stored in a manner to be included in the regular backup process per the "IT Disaster Recovery and Business Continuity Policy." This standard seeks to avoid major data losses and the consequences that result in the event of a disaster or unavailability of the system. Each department must determine the back-up frequencies. Some systems will need to be backed up more often than other systems. The criticality of the data and data-type are important factors to the back-up frequency.

References

- Home Connection Reimbursement Policy
- IT Security Policy
- IT Facilities Security Policy
- Data Investigation Policy
- Business Computer Equipment Policy
- Email/Electronic Communications Policy
- IT Disaster Recovery and Business Continuity Policy
- Purchasing Information Technology Related Items Policy
- Information Technology Committee Policy
- Internet Access and Use Policy
- Information Technology Employee Information Access Policy
- PC Disposal Policy & Form

EMAIL/ELECTRONIC COMMUNICATIONS POLICY

Summary: *This policy assures the proper use of electronic communications, including electronic mail (email), text messaging, and other messaging/communications solutions, for authorized purposes by County employees within the parameters described in this policy.*

DEFINITION OF TERMS

Electronic Communications System: Any system, or tool used to send, or receive messages, or other records between recipients, including but not limited to Microsoft's Exchange, Office 365, email provided by a web browser, or text messages.

Electronic Records: All information transmitted, or stored by electronic communications systems, are considered electronic records, and are subject to the County's record retention schedule, and the Public Records Act (RCW 42.56).

POLICY

The County's electronic communications systems are to be used primarily for official County business purposes. The use for other than County business purposes is expected to be limited and restricted by the parameters provided within this policy. Users of these systems will comply with all applicable laws and policies, including but not limited to those related to Information Technology security, privacy and public records.

STANDARD

This Policy applies to employees, or others, who use or may have authorized access to Pierce County's computer or communications systems.

PROCEDURE

PERSONAL USE OF ELECTRONIC COMMUNICATIONS SYSTEMS

Occasional and incidental personal use of electronic communication systems by authorized users may be permitted on a limited and brief basis where use of the system is not done in a manner that impacts work time or negatively affects the workplace. It is expected that such use will be conducted using good judgment and with the knowledge that we are accountable to the taxpayers. In addition, authorized users must understand that such use comes with the implicit and express consent of the user for the County to monitor, access, use, and disclose electronic records. Such use must not violate other County policies (e.g., soliciting items for sale, harassment, Internet Access and Use Policy, use for private business, misuse of County time, etc.). See also "Prohibited Uses" in this policy. If an authorized user wants to send an email and they are uncertain about whether it is permitted under this policy, the matter should first be discussed with their supervisor.

ELECTRONIC RECORDS ARE NOT PRIVATE

The electronic communications systems have been provided by the County to facilitate County communications and business. The electronic records stored and transmitted by these systems are considered to be the same as any other County paper document, and as such are the property of the County. The County reserves the right to monitor, access, use, and disclose email and other electronic records. Additionally, unless those communications deal with matters exempted by state law, they are considered to be "public records" and not private or personal. As with all information contained on County computers/equipment, no one has a right to privacy in any matter created, received, stored, or sent on the electronic systems.

Extra care should be taken when communicating protected information as defined in the IT Security Policy. Communications may also contain sensitive or confidential or proprietary business information. In such cases, other, more secure means of communication should be employed to avoid any risk of disclosure, especially considering that electronic records sent over the internet may become available to anyone on the internet. County systems do not control forwarding of an email or other electronic information.

USE OF EMAIL

Email records stewardship: Email sent and received by Pierce County users are associated with the department they work for and as such fall under the records management plan and data investigation stewardship of that department. Existing or returning Pierce County users hired into new positions in a different department will retain the same login name and email address but will not have access to email in their prior position. If appropriate, access to email in their prior position can be requested through the Data Investigation Policy requiring approval from their previous department head.

Frequency for Reading Email: In order to make email effective, users are to check their email at least once per day, and to respond as appropriate in a timely manner.

Global Messages: Countywide messages may only be used by the County Executive's Office, the Communications Department, email administrator, and other authorized individuals, or groups approved by the County Executive's Office, and only for Executive-sanctioned purposes. Requests for global messages should be forwarded to the Executive's Office.

Official County Business: In order to meet our records retention requirements, all email communication used to conduct official County business shall be performed using the County's official email system not a secondary communication system such as external instant messaging, or a web-hosted or third-party email account.

- Pierce County email accounts will be provided to County employees and approved volunteers that need this functionality to complete their County business job duties.
    - Outside agencies with Online Services Agreements with Pierce County Information Technology may be provisioned with County email accounts by contract but must use a naming standard that clearly indicates their agency name so these emails are recognized as not being official County business.
    - Outside agencies that partner onsite with Pierce County to provide improved services to citizens will only be provided with Pierce County email accounts if they are unable to use their agency email address to complete the functions of their partnership with Pierce County. Their email address name or email signature block needs to clearly indicate that they are a Pierce County agency partner.
    - Pierce County contractors will only be provided with Pierce County email accounts if they are unable to use their company email address to complete the functions of their contract with Pierce County. Their email address name or email signature block needs to clearly indicate that they are a contractor of Pierce County and their role in representing Pierce County through the use of this email account.

Protected information: Email users need to be careful with the distribution of protected information, such as that regulated by the Health Insurance Portability and Accountability Act (HIPAA), the Criminal Justice Information Services Security Policy (CJIS), and the Payment Card Industry Security Standards (PCI). Protected information should generally not be sent via email unless necessary. When protected information is sent in email, the email communication should be encrypted. Email sent and received between users on the Pierce County network is encrypted automatically. Email sent to external parties is not encrypted by default, however a function to encrypt outgoing email is provided and should be used if protected information must be sent in email.

Retention:

- Email: Upon send or receipt, email is automatically included in the County's email repository and retained according to the County's Email Retention Policy.

- Calendar Appointments, Tasks, Contacts: Automatically included in the County's email repository and retained according to the County's Email Retention Policy.

Security: In order to safeguard Pierce County computer systems and information assets, email users are expected to use good judgement and extreme caution when receiving unsolicited email because it may contain an attachment or link that if opened could inflict harm to Pierce County. If unsure, users should either delete the message or contact the IT Service Desk.

USE OF NON-EMAIL COMMUNICATIONS SYSTEMS

Other forms of electronic communications systems are subject to the same policies as email. However, there are no automated solutions in place to backup, archive, retain, and disclose the electronic records created through the use of these systems. It is the user's responsibility to take the appropriate actions to meet the legal and policy requirements associated with those records.

PROHIBITED USES OF ELECTRONIC COMMUNICATIONS SYSTEMS

The following are provided as examples of prohibited uses and are not intended to be all inclusive. Users are prohibited from sending, accessing, downloading, viewing, receiving, or possessing materials which would generally be considered to be inappropriate in the workplace. This includes any material of a sexual nature such as jokes, posters, pictures, or sexual communications. In addition, communications which would be inappropriate under other policies are also prohibited (e.g., sexual harassment, racial comments, religious or political solicitations, insubordination, breaches of confidentiality, dealing with illegal activity, etc.) Other examples of prohibited uses include: use for personal or commercial gain, chain-letters, sending junk mail, bypassing security systems, attempting to cause harm to another computer system, actions which violate copyright or trademark laws, or other license restrictions. Users are responsible for notifying individuals from whom they receive inappropriate or excessive electronic communications to immediately discontinue such use of the system.

Users who are unable to resolve unsolicited or inappropriate electronic communications themselves, should immediately notify their supervisor or the system administrator when receiving unsolicited, inappropriate communications so they can assist in preventing such communications.

Users are prohibited from creating automated forwarding rules that send received electronic communications to an external address. Forwarding messages in this manner creates excess traffic, may cause confidential or other sensitive County information to be transmitted and stored in an unprotected manner outside our organization, or may be blocked due to its spam-like behavior. Occasional forwarding of an individual, non-sensitive message is permitted on a limited basis as long as it does not impact work time, negatively affect the workplace, or put sensitive data at risk.

The County shall consider a variety of factors when determining if there has been prohibited use of the County's computer system including, but not limited to the: 1) extent of use; 2) frequency of

use; 3) sites accessed; 4) parties corresponded with; 5) time spent; 6) impact or potential impact on the County; 7) potential risk of exposure to the County; 8) content or purpose of the message.

Disciplinary Action for Misuse: The County considers misuse of its computer systems to be a serious matter. Failure to follow this policy may be grounds for disciplinary action, up to and including discharge.

Effective: *February 1, 2019*
Last Revised: *April 1997*
March 2004
November 2004
July 2006
April 2009
June 2010
August 2015
References: Internet Access and Use Policy and Email Retention Policy

BUSINESS COMPUTER EQUIPMENT POLICY

Summary: *This policy maximizes business computer up-time and ensures business continuity for Pierce County services by utilizing proven, cost-effective best practices in computer technology support methodologies.*

Definition of Terms

Business Computer: Desktop PCs, laptops, tablets, smartphones, and other similar user access and interface devices owned by Pierce County.

Business Computer Equipment: All the above plus peripheral equipment such as printers, plotters, web cameras, scanners, etc.

Disk Imaging Software: Software used to copy the entire contents of a computer's hard drive.

Endpoint Management: Software tools, policies, and rules used to remotely configure and maintain business computers including distribution of software, patches, and security protection layers.

IT: The Information Technology Division of the Pierce County Finance Department.

IT IO Unit: The IT Infrastructure and Operations Unit that administers business computer equipment.

IT Computer Asset Management System: An application to track hardware and software inventory for Pierce County.

IT Security Team: A team of IT staff, comprised of the Assistant Director of IT, IT Security Officer, all IT Managers, and expert Systems Engineers from every major discipline area, who provide governance functions that support Pierce County's cybersecurity responsibilities.

Computer Lifecycle Program: An IT program that provisions desktop or laptop County standard computers for workers requiring computers to perform their work. It also provides for in-service shared, kiosk, and common use computers. The computers are assigned to a "refresh cycle" which will determine which subsequent year each will be replaced.

PC Lifecycle Program: An IT program that provides centralized management for Pierce County computer hardware. This program oversees the planning, procurement, deployments, maintenance, and replacement at the direction of the IT IO Unit.

PC Lifecycle Group: Contracted technicians and administrative staff that conduct equipment installations, repair, and disposal at the direction of the IT IO Unit.

Security Software: Software running on a computer with the purpose of protecting the computer from security risks. Security software includes antivirus protection, spyware protection, firewall protection, zero-day defense protection, etc.

Standard Images: IT configured and tested startup configuration for each County standard business computer model.

Standard Security Software: Security software mandated to run on devices as a cybersecurity layer of protection.

Technology Coordinator: An official, approved and assigned role in County departments that act as a partner for IT in providing successful computing environment support and planning services for their department. Additionally, the role submits new and departing user requests, orients new employees, and conducts tier one troubleshooting.

Policy

Acquisition
The Computer Lifecycle Program provisions desktop and laptop computers to County workers and replaces those computers according to a predefined refresh cycle. For other business computer equipment, the Pierce County Purchasing Policy, as described in the Finance Policy and Procedures Manual, mirrors the Information Technology Purchasing Policy which states that business computer equipment acquisitions require approval by Information Technology. This review is to ensure compatibility with existing infrastructure investments, to utilize established standards and best practices to the benefit of County operations, and to save County resources. IT focuses on providing responsive, cost-effective support for County standard hardware and software. Occasionally, IT will approve a non-standard purchase where no standard exists or where IT agrees there is benefit to the County. In these cases, hardware and software support agreements will need to be prepared prior to the purchase approval. IT will centrally manage a computer hardware acquisition contract for standard business computers and business computer equipment.

Deployment, Maintenance, Disposal
Business computers and equipment will be deployed and repaired through the PC Lifecycle Program. IT will manage the contract and the contractors required to provide these services. Maintenance for specialized devices such as plotters and high-end scanners and other specialized equipment will require separate maintenance contracts to be purchased and managed by the equipment owner. Computer equipment is to be disposed of through the PC Lifecycle Program to ensure proper data erasure occurs and to ensure that it is disposed of in an environmentally safe manner. Please refer to the PC Lifecycle procedures for more details on this program.

Best Practices for Endpoint Management
All County business computers will follow these best practices adopted by Pierce County:

1. Business computer purchases must be one of the standard model choices, or an alternative, approved by IT.

2. The operating system for each standard model will be determined by IT. Unless an exemption is approved from IT, the initial assigned operating system will not be upgraded to any new version except for service pack releases.

3. Business computers will be deployed using IT standard imaging techniques, include all IT standard security software and will utilize all standard endpoint management tools.

4. Business computers will reside in the County's Active Directory 'CountyComputers' OU (organizational unit) for device security and management, unless there is a specific exemption approved by the IT Security Team.

5. Business computer configurations will follow all Information Technology Security Policy standards, unless a specific exemption is approved by the IT Security Team.

6. Wherever possible, devices will be configured to conserve energy through standard configuration settings or centrally controlled software managed by the IT IO Unit.

7. Unless otherwise approved by the Assistant Director of Information Technology, only IT staff and authorized Technology Coordinators are provided with local administrator privileges needed to install approved software on Pierce County business computers.

Software

Pierce County business computers will only run standard County software packages or other software developed or approved by IT. Pierce County employees may not use an alternate software package to meet their personal preferences.

Only software licensed to Pierce County and approved by IT can be used on Pierce County owned business computers. Exceptions may be provided for software licenses being used under a valid evaluation program, a consultant legally using their software license on a County business computer to complete work for Pierce County, and other approved, work-related, legal use of software licenses.

Software personally owned by Pierce County employees cannot be installed on Pierce County owned business computers. Ownership of personally owned software can be permanently transferred to a Pierce County department with owner and department management documented approval.

Pierce County employees will comply with the terms and conditions of software license agreements and no employee may, or may be asked to, install software on business computers owned by Pierce County that violate a licensing agreement. IT will maintain proof of license ownership for software licenses owned by IT for use on County computers. County departments are responsible for maintaining proof of ownership for all software licenses they own and operate in their environment. These documents should be kept in an organized fashion, readily available for an auditor to access when a software compliance audit occurs.

Pierce County employees will not download or otherwise make copies of copyrighted software or other copyrighted materials without permission from the copyright owner. As such, downloading or

copying of unlicensed software, music files, photographs, clipart, etc. which violates copyright laws is explicitly prohibited. Please refer to the Fair Use Policy.

Pierce County employees will not download or install any software, even if considered "free," to Pierce County business computers without approval from IT. This restriction includes entertainment and personalization software that employees may not see as licensed software needing approval. These programs often contain viruses, spyware, as well as other hidden threats; can put County data at risk; can interfere with the successful operation of legitimate County software used to run County operations; or can open a security risk to the entire County network. Employees need to be aware that fixing business computers broken through personalization or personal software preference incurs costs. As such, IT staff are directed to report violations of this section of the policy to the employee's management as well as the Human Resources Department.

Unless an established, supported standard solution, Pierce County employees will not sign up for or use any web-based/cloud/software-as-a-service (SaaS) applications, even if considered "free," without approval from IT. As with locally installed applications, these web-based applications can interfere with the successful operation of legitimate County software used to run County operations or can open a security risk to the entire County network. Wherein any County business record is stored or generated within the web-based application environment, that environment becomes subject to all business record management, public disclosure, security, and vendor management policy and requirements.

Connectivity
County owned standard business computer equipment needing access to central systems will be connected to the Pierce County internal network according to IT standards. Non-standard County owned business computer equipment can only be connected to the County network after a security review and with the explicit approval from the IT Security Team. Personally owned computer equipment is expressly prohibited from being connected to the Pierce County internal network. IT reserves the right to immediately terminate any unauthorized or problematic network connection.

Asset Management
To comply with Pierce County Code, business computer equipment purchased by the County will be entered into the IT Computer Asset Management System by the IT IO Unit (following confirmation of equipment receipt through vendor report, packing slip, or voucher payment). County departments are required to partner with the IT IO Unit to maintain an accurate business computer equipment inventory through the use of the centralized IT Computer Asset Management application. Real time asset tracking is accomplished through various operation management systems. Any tracked equipment asset that is in service and reported through the operational management systems is considered part of the inventory. County departments will work with IT annually to reconcile any instances where the asset management system shows tracked assets that are not reporting in through the operational management system. All lost equipment will be reported per Finance Department procedures. County departments wishing to dispose of business computer equipment shall follow the PC Lifecycle PC Disposal process.

Backups
Saving County data on local computer hard drives is not recommended. Pierce County data should always be stored on approved file storage services like the M: or N: drive where data is safeguarded through routine backup processes. Business computer equipment hard drives are not backed up because it is expensive and logistically difficult. These devices can easily be restored to default

settings in case of failure. If an employee chooses to store County data on their local computer hard drive, or other removable media, the employee must take responsibility for safeguarding the data by performing routine backups themselves.

Personal Use
Unless explicitly stated in a separate policy such as the Email/Electronic Records Policy or Internet Access and Use Policy, employees are prohibited from using County business computer equipment for personal reasons. These uses include creating personal use files, downloading software for personal enjoyment or preference, storing music or movies on their computer hard drive, maintaining financial records, purchasing personal use items, etc. An acceptable exception is the use of a personally owned photo for desktop 'wallpaper' purposes.

Other
The contents of County business computers are not private and can be reviewed at any time by County management or their representatives up to and including removal of the business computer for investigative purposes.

Please refer to the Information Technology Security Policy for additional requirements employees need to follow to help secure Pierce County electronic assets.

Effective:	*February 1, 2019*
Last Revised:	*April 2008*
	July 2006
	January 2006

References:
IT Security Policy, Internet Access and Use Policy, Email/Electronic Records Policy, Email Retention Policy, and
Fair Use Policy

INTERNET ACCESS AND USE POLICY

Summary: *This policy defines allowable and appropriate uses of the internet.*

DEFINITION OF TERMS

Business Computer: Desktop PCs, laptops, tablets, smartphones, and other similar user interface devices owned by Pierce County.

Business Computer Equipment: Refers to all the above plus peripheral equipment such as printers, plotters, digital cameras, web cameras, scanners, etc.

POLICY

Internet Access

Filtered and logged internet access is available to any user on the County's internal network by default. A department director, or their designee, can explicitly deny internet access for a particular user or computer by request to Information Technology. To enable certain specialized job functions, a department director may authorize, in writing to Information Technology, unfiltered internet access for particular employees.

Access to the internet from any business computer connected to the County's internal network is only allowed via the County's centralized internet connection. Requests for exceptions to this rule must be reviewed and approved by the Assistant Director of Information Technology.

Internet Use

All Pierce County employees are responsible for using internet resources in an ethical, responsible, and legal manner. The primary use of the internet via Pierce County business computers will be for County business related purposes. Department directors are responsible for managing use of the internet by their staff, restricting use or limiting time as they see appropriate. Users should consider their internet activity as public information and manage their activity accordingly. All internet traffic goes out beyond the protected Pierce County network into a wide-reaching unsecure network. Information Technology monitors and reports on the internet activity on the County's network.

Personal Use

As a benefit to employees, internet access for personal use by authorized users may be permitted on a limited and brief basis where use of the system is not done in a manner that impacts work time or negatively affects the workplace. It is expected that such use will be conducted using good judgment, with the knowledge that employees are accountable to the taxpayers and that personal

internet access directly competes for limited resources used to conduct legitimate County operations and provide the public access to our on-line government services. Employees will be held responsible for their internet usage.

This limited personal use of the internet is intended to allow employees incidental, unplanned, but necessary access to information needed during the workday, similar to the use of a County phone to make a brief personal phone call. These access periods are intended to be quick, as in less than five minutes, and to be specifically targeted activities rather than just looking around the internet to pass the time on break. Such activities may not be done during work time. Please refer to the more detailed "Frequently Asked Questions: Personal Internet Use" document referenced later in this policy for more information.

Authorized users must understand that such use comes with the implicit and express consent of the user for the County to monitor, access, use, and disclose activity. Such use must not violate other County policies (e.g., soliciting items for sale, discrimination, harassment, use for private business, misuse of County time, etc.). See also "Prohibited Uses" in this policy. If an authorized user wants to access an internet site and they are uncertain about whether it is permitted under this policy, they should first read the "Frequently Asked Questions: Personal Internet Use" document referred to in the reference section of this policy matter. If questions remain, they should discuss them with their supervisor. Users must understand that all personal use of the internet via County resources is at their own risk and precautions necessary to protect their privacy and sensitive information is their responsibility.

Prohibited Uses

The following are provided as examples of prohibited uses and are not intended to be all inclusive. Users are prohibited from accessing, downloading, or viewing materials which would generally be considered inappropriate in the workplace. This includes any material of a sexual nature such as jokes, posters, pictures, or sexual communications. In addition, communications which would be inappropriate under other policies are also prohibited (e.g., sexual harassment, racial comments, religious or political solicitations, insubordination, breaches of confidentiality, dealing with illegal activity, etc.). Other examples of prohibited uses include: use for personal or commercial gain, social media, chat rooms, bypassing security systems, attempting to cause harm to another computer system, viewing or using bandwidth intensive activities, actions which violate copyright or trademark laws, or other license restrictions. Employees are responsible for understanding what use is not acceptable and should read the "Frequently Asked Questions: Personal Internet Use" document referred to in the reference section of this policy.

The County shall consider a variety of factors when determining if there has been prohibited use of the County's computer system including, but not limited to the:

1) extent of use
2) frequency of use
3) sites accessed

4) parties corresponded with
5) time spent
6) impact or potential impact on the County
7) potential risk of exposure to the County
8) content or purpose of the message

Effective:	*February 1, 2019*
Last Revised:	*November 2010*
	January 2007
	July 2006
	April 1999

References:

Frequently Asked Questions: Personal Internet Use

Is personal use of the internet allowed?

Yes. The County's Internet Access and Use Policy says, "personal use by authorized users may be permitted on a limited and brief basis where use of the system is not done in a manner that impacts work time or negatively affects the workplace."

Why?

The County agrees to provide Internet authorized employees with this service as a benefit to address the occasional issue that arises during work where the Internet is the best method to handle it quickly. We are all busy people and we know this will help employees. We can offer this benefit as long as it is not abused in a way that negatively affects County operations or work time.

Are there limitations about what I can access for my personal use?

Yes. The County's internet connection is **not** meant to provide your primary internet access method for conducting personal business, reading news, completing online shopping, etc. As a rule of thumb, if the Internet access can wait until you are off work, then wait until then, rather than using County resources for your personal business.

There are particular personal internet activities which, even if quick, should be avoided to limit the negative impact on County operations. Specifically, bandwidth intensive activities and those with an accompanying security risk must be avoided.

Examples of bandwidth impacting activities that should be avoided include:

- Watching/streaming live video.
- Subscribing to web services that automatically send you updated information on a regular basis such as weather, sports scores or stock tickers.
- Transaction-oriented activity such as shopping, participating in online auctions, planning vacations, and managing personal finances online.
- Streaming radio station feeds or music sites like Pandora or Amazon Music.

As far as security risks go, accessing web pages including internet email can expose the County to risk of virus infection if you open a web page that automatically executes a program or links to an infected file or attachment you choose to open. Please be cautious before opening any web page from an unknown source.

Any activity that violates other County policies, codes, or guidelines is prohibited. In particular, employees should not access the internet at work for any activity related to generating revenue such as running their own business.

I can use the phone on my desk for local personal calls, why are there more restrictions on personal internet use?

There actually are some restrictions on the use of County telephones. Personal internet use cannot be billed to staff but because all internet traffic coming in and out of the County goes through the same "pipe." Everything competes for the limited pipe size, so we should limit personal use. While you are using the internet at work for personal activity, you are sharing the limited bandwidth with the public looking to pay property taxes, private lawyers completing court activities online, employees using internet resources to complete their work, partner agencies using our website information to help citizens, the public looking up court case information or permit status, etc. If you are connected to the internet at home, you probably pay $30-$50 a month for this service. Internet connectivity for businesses is much more expensive. The County currently pays over $5,000 a month for our internet service and, we do not want to incur even higher costs by allowing employees to utilize unlimited internet resources for their personal benefit.

What are examples of what I am allowed to use the internet for personally?

Examples of acceptable personal internet use:

- Obtaining directions from an online mapping service to figure out how to drive by a particular store on the way home from work.
- Checking the status of an incoming flight for someone you are picking up at the airport leaving directly from work.
- Checking the loan rates at Tapco.com instead of making a phone call.
- Looking up phone numbers; or checking the hours of a store you want to stop by on the way home.

This is by no means an all-inclusive list, but it gives you the idea that the County recognizes the value of the internet as an information tool for busy working people that can make them more efficient overall.

What are some important considerations to remember if I do use the internet for personal use?

All internet access on County computers is logged. This information can be reviewed as part of an employee investigation and/or released as a part of a public records or litigation request. All personal use of the internet via County resources is at your own risk and precautions necessary to protect your privacy and sensitive information are your responsibility.

I prefer to use my personally owned laptop or smart phone (a personal internet device) for accessing the internet while at work. Are there any issues with that?

Use of personal internet devices such as laptops or smart phones using a public wireless access point, or your own funded wireless internet access plan is currently allowed but must be limited so it does not negatively impact your work time. Such use must be on your break or lunch time and should not violate any County policies or prohibitions such as viewing offensive material around others. Also, be sensitive to the County's sustainability initiatives and avoid plugging in personally owned computers or charging personal smart phones at work.

What if I'm still unsure if a particular action is ok?

If this document has not addressed a specific question about whether a particular use is permitted under the Internet Access and Use Policy, the matter should first be discussed with your supervisor.