Seattle
Information Technology

INFORMATION TECHNOLOGY SECURITY POLICY

POLICY 201

Purpose

The purpose of this document is to define a policy that helps ensure the security, availability and productive use of City of Seattle Information Technology systems and networks. It also helps ensure the confidentiality, integrity and availability of electronic information captured, stored, maintained, and used by the City of Seattle. It provides direction for compliance to federal and state regulations, specifies appropriate practices, and defines custodial responsibilities for records associated with City operations. This policy, as a whole or in component parts, should be used as a foundation document for all additional policies, standards, procedures, and guidelines that are developed and implemented by the City related to information systems security.

All Users of City computing services, resources and data are required to support this effort by complying with all established policies, standards, guidelines and procedures. This includes compliance with all related federal and state statutes and regulations as required.

Scope

This Policy is applicable to all users (including all employees, elected and appointed officials, contractors, vendors, volunteers and others) and departments of City Information Technology (IT) systems, networks, devices, digital information, and any other electronic processing or communications related resources or services provided through the City.

In Scope

General IT systems operated and maintained by ITD and available to all City Users

Out of Scope

IT systems operated and maintained by city departments may have their own sets of policies that supersede these policies. These policies shall apply unless other policies specifically meet or exceed them

Departmental Operations Technology (OT) systems

Policy

A. ACCEPTABLE USE

Acceptable Use

This defines the appropriate use of technology resources and data that are owned by the City of Seattle and provided for employee use. Departments may issue their own policies that augment or adopt this policy through reference, but not to supersede or contradict it.

1. City Resources are for City Business

City-owned technology resources shall serve the business needs of the City of Seattle

2. No Expectation of Privacy:

Employees must not expect privacy in the use of City communications and digital equipment. Nothing in this policy confers an individual right, or shall be construed to provide, an expectation of privacy.

3. Confidentiality:

City-held information on the constituents of the City of Seattle shall not be accessed or disclosed without a clear business need and authorization (including, but not limited to Public Disclosure Request).

4. Limited Personal Use:

City-owned technology resources may be used for personal purposes on a limited basis, providing this use results in:

- No marginal cost to the City
- No interference with work responsibilities
- No disruption to the workplace
- No storage of unlicensed, copyrighted materials on any City owned technology resources.
- No device-to-device connection of non-City-owned technology resources to City-owned technology resources. For example, charging of personal smartphones via City computer USB port is prohibited.
- No illegal activities.
- No commercial or solicitation activities.
- No use of internet or messaging tools for activities that are listed under “Specific Prohibitions and Limitations”.

5. Limited use of external e-mail services:

The limited use of an external email service is allowed, providing that the service applies anti-malware controls in a manner equivalent to that provided by the City, and such use is incidental and does not interfere with City workload, as determined by your supervisor. Attachments and embedded links should not be clicked or downloaded.

6. Media Files:

City computers, devices, and other storage locations must not be used to download or store music/audio/movies/eBooks/games files for personal use.

7. Sharing of City Data Files:

City data files may be shared as needed to support City functions and in accordance with the Information Technology Security Policy, in particular:

7.1 Data files classified as PUBLIC may be shared without restriction except where copyright is applicable.

7.2 Data files classified as SENSITIVE shall be shared only when the City has a documented business need, or to meet legal requirements, including the Washington Public Records Act pursuant to specific public disclosure requests. Restricted data files should be shared only when the integrity and obligations of the City's business operations and compliance requirements are ensured.

7.3 Data files classified as CONFIDENTIAL should not be shared except as required to conduct City business, or to meet legal requirements. It is specifically protected in all or in part from disclosure under the State of Washington Public Disclosure Laws.

7.4 Data files classified as CONFIDENTIAL REQUIRING SPECIAL HANDLING is specifically protected from disclosure by law and subject to strict handling requirements dictated by statues, regulations, or legal agreements.

7.5 For additional guidance see GUI110 Data Classification Guideline or consult department specific data classification and policies for additional restrictions where applicable..

8. Downloading to and Storage of City Records on Non-City-owned Technology Resources:

Data files with restricted classifications shall not be downloaded to, nor stored on non-City-owned technology resources. Exceptions may be granted for SENSITIVE and CONFIDENTIAL with approval from Departments or the Digital Security Governance Committee. Data classified as CONFIDENTIAL REQUIRING SPECIAL HANDLING must adhere to regulatory standards and may not be stored on non-City owned technology.

The use of removable media shall be restricted to authorized users, consistent with the Removable Media Standard.

City or public records stored on non-City-owned technology resources must be retained and produced in accordance with legal requirements, including but not limited to Washington State records retention laws and the Public Records Act.

9. Specific Prohibitions and Limitations:

City policies regarding acceptable behavior and communication will apply to use of the Internet and messaging. Specifically prohibited use includes, but is not limited to:

9.1 Conducting a private business;

9.2 Political campaigning;

9.3 Accessing sites which promote exclusivity, hatred, discrimination or exclusionary positions which are contrary to the City’s policy of embracing cultural diversity;

9.4 Accessing inappropriate sites including adult content, online gambling, online gaming, and dating services;

9.5 Accessing sites that promote illegal activity, copyright violation, or activity that violates the City’s ethical standards;

9.6 Using the internet to obtain or disseminate language or material which would normally be prohibited in the workplace;

9.7 Using encryption technology that has not been approved for use by the City;

9.8 Making unauthorized general message distributions to all users (everyone);

9.9 Installing any software that has not been approved by the City or unless approved through exception process by management in consultation with authorized IT representatives;

9.10 Sharing or storing unlicensed software or audio/video files;

9.11 Using unauthorized tools to attempt to elevate user privileges, obtain unauthorized resources, disrupt availability or make unauthorized alterations;

9.12 Broadcasting e-mail to large numbers of external constituents unless the list members are hidden through the use of the BCC field.

9.13 Using a City e-mail address when posting to public forums e.g. blogs, social media sites, wikis and discussion lists for personal use;

9.14 Use of online shopping and/or interferes with your workload, as determined by your supervisor;

9.15 Excessive use of social media sites for personal use (as described in "Limited Personal Use") that is more than incidental, and/or interferes with your workload, as determined by your supervisor;

9.16 Use of streaming media for other than City of Seattle business purposes during work hours;

9.17 Using unauthorized Peer-to-Peer Networking;

9.18 Using a City e-mail address as a means of notification for personal use, e.g. shopping, dating or social media sites.

- ➢ If any of the above prohibited uses is required for a legitimate business reason, it is management's responsibility to follow the Seattle IT Exception Process.

10. Use Standard Resources Only:

All digital equipment and applications must be authorized. Only software, hardware, cloud services, and communication protocols that meet the City's defined standards will be installed on, or connected to, City-owned technology resources unless an exception has been granted according to the exception process. Also do not alter to remove approved standard software from City-owned Technology Resources.

11. Additional Cost to the City:

Resources that incur a cost to the City, whether accessed via the internet, mobile device, email or other applications, must not be accessed or downloaded to any City-owned technology resources without prior approval. It is the supervisor's responsibility to assure the business need, applicability, and safety of any new resource.

12. Conflicts:

If any component of this policy conflicts with any applicable collective bargaining agreement, the collective bargaining agreement shall control. The remaining non-conflicting features of this policy shall remain in effect

Smartphone and Mobile Device Policy

13. Smartphones

The use of smartphones and mobile devices connected to City resources is based on the needs of the business and subject to departmental approval.

13.1 Employees will adhere to City data retention policies and schedules for all City business records that reside on City-owned or employee-owned smartphones or other mobile devices

13.2 Employees using a City-owned device will comply with all applicable City and departmental policies and workplace expectations while using the smartphone or mobile device.

13.3 City information stored on City-owned or personal smartphones or other mobile devices is a public record subject to disclosure pursuant to the provisions of the Public Records Act, RCW Chapter 42.56 ("PRA"). It is the responsibility of each City employee to retain public records, including those on City-owned or personal smartphones and mobile devices. Retention of text messages is based on the content of the message and the function it documents, not the method of transmission.

14. City Owned Devices

14.1 There is no expectation of privacy when using City-owned smartphones and mobile devices. The City has the right to review all mobile device records including, but not limited to, phone logs, text messages, photographs, installed apps and internet usage logs.

14.2 Employees should avoid using City-owned smartphones and mobile devices to send or receive personal text messages. When the City receives a public disclosure request, a discovery request in connection with litigation, or other form of request to which it is legally required to respond, records on a City-owned device must be retained until the City responds to the request. Personal records on a City-owned mobile device may potentially be disclosed in response to any request to which the City is obligated to provide records.

14.3 Employees should download only applications necessary to conduct City business in compliance with departmental policy and/or City policy.

14.4 Passwords are required on City-owned smartphones and mobile devices to connect to City resources. The password is to be managed in accordance IT policy.

15. Personal Devices

15.1 Employees using a personal device will comply with all applicable City and departmental policies and workplace expectations while using the smartphone or mobile device for City business.

- ➢ City employees must use private internet connection such as home networks and avoid conducting City business over public Wi-Fi such as those found in a coffee shop or library (unless using a VPN).
- ➢ City employees should have the most current antivirus software and security updates possible for their personal devices and should be cautious when using personal devices/computers that are shared with family members to reduce their vulnerability to a cyber-attack.

15.2 City staff shall not create, capture or store data that is classified as "Confidential" or "Confidential - Special Handling" on a mobile device unless there is a secure app or Mobile Device Management solution on the device that ensures the security of that data in the event that the device is lost or otherwise accessed by unauthorized parties.

15.3 City Staff should not store City data on a personal device, storage media or file storage service.

15.4 If City data is inadvertently stored in personal device (including mobile devices), records must observe record retention requirements and be retained for the applicable retention period. Employees should consult the City Records Management Program for retention requirements.

15.5 An employee who uses a personal mobile device for City business is required to follow this policy and to cooperate with the City and provide fullest assistance in fulfilling the City's duties and obligations under the Public Records Act.

15.6 Employees shall provide all records created, received, or retained within the scope of their employment on a personal mobile device to the department's PDO in response to a public records request. This includes records required by the Employee's position/function, records the Employee is directed to have by the City, or records created, received, or retained in furtherance of the City's interests. Employees may be required to sign an affidavit describing the search process used to identify public records stored on the personal mobile device and stating that all responsive records have been provided to the City.

15.7 If an employee-owned smartphone or mobile device that contains City records or data is lost, stolen or broken the employee must notify their immediate supervisor within one business day.

15.8 Employees who use personal smartphones or mobile devices to conduct City business are required to use a personal password to protect the entire device.

15.9 Users who use personal systems to access the City Network for work purposes must adhere to and Systems and Network requirements and must maintain up-to-date security software as follows:

- Current Operation System (OS) and security patch level
- Firewall enabled
- Current version of antivirus software with an up-to-date signature
- VPN where appropriate

15.10 City Data is not to be stored on personal laptops or other personal systems used to access the City Network

15.11 Any non-approved (including tablets or any non-approved IoT technology) may not in any way be connected to the City's authenticated network.

B. ACCESS CONTROL & ACCOUNT MANAGEMENT

Account Management

In accordance with the principle of least privilege, account types are established with specific privilege levels required to perform prescribed functions. Standard user accounts are the default user account used for all general operations not requiring elevated privileges.

All Users' system access will be based on the "principle of least privilege" and the "principle of separation of duties”:

16. Principle of Least Privilege:

An operations principle that requires access privileges for any user to be limited to only what they need to have (nothing in addition) and when they need to have it, to be able to complete their assigned duties or functions. The IT Department shall:

- Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- Authorize explicit access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.
- Require that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions.
- Restrict privileged accounts on the information system to authorized individuals only; and only for the periods they are authorized
- Ensure that the information system audits the execution of privileged functions.
- Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
- Should not copy or clone account or file privileges from existing end-user or admin accounts.

17. Principle of Separation of Duties:

- An operations principle that requires that whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm. The IT Department shall:
  - Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
  - Document the separation of duties of individuals.
  - Define information system access authorizations to support separation of duties

18. Provisioning

18.1 Computer applications that are developed for the system must be developed and integrated to maintain individual user accountability and audit capability.

18.2 Documented procedures must be in place for issuing access, access change, access termination and revoking access privileges on systems and accounts.

18.3 A formal process rigorous enough to withstand after-the-fact audit scrutiny is required for deprovisioning access whereby the employee's supervisor initiates a procedure in ServiceHub whenever an employee departs from their group to ensure HR is informed and appropriate access is removed whenever:

- Accounts are no longer required;
- Accounts are inactive for a defined period of time;
- Users are terminated or transferred; or
- Individual information system usage or need-to-know requirements changes.

18.4 Any vendor that requires access to City equipment must obtain written permission from departmental IT Management.

- Enable vendor accounts used for remote maintenance only when actively being used by the vendor and disable the access upon completion of vendor activity;
- Audit vendor accounts used for remote maintenance on a periodic basis to ensure access is being disabled when not actively in use;
- Change vendor-supplied defaults (including passwords) and remove or disable unnecessary default accounts before installing a system on the network;

19. Monitoring of User Accounts, Files, and Access

19.1 The City reserves the right to monitor its information systems and user activity. There is no guarantee of privacy of email, Internet access, system logs, and electronic files related to individual City computer and network accounts.

19.2 Inappropriate, unauthorized use or abuses of computing and network resources are subject to monitoring and investigation by authorized City staff.

19.3 Individuals and associated accounts under investigation are subject to having their activities on City systems monitored and recorded.

19.4 In the course of monitoring individuals who are improperly using these systems, or in the course of correcting system problems caused by the unauthorized use, the activities and files of authorized users may also be disclosed.

19.5 The City may specifically and without notice monitor the activity and accounts of individual users including files, session logs, content of communication and Internet access for adherence to the Acceptable Use Policy.

19.6 The City reserves the right to filter Internet access to preclude dangerous or harmful connections.

19.7 Evidence of criminal activity will be turned over to appropriate City and law enforcement officials.

Administrative Access to City Information Systems

Administrator (and other higher privileged) accounts are used to establish separate elevated privileges required to perform specific systems management functions.

20. Appropriate Use of Standard User Accounts

20.1 Standard user accounts must be used for accessing common business applications and performing daily work where elevated rights are not explicitly required.

20.2 Standard user accounts will not be used to perform administrator system functions.

21. Appropriate Use of Elevated Privileged Accounts

21.1 Appropriate use of administrator accounts includes managing applications, infrastructure, network devices, operating administrative tools, or performing other essential management or administrator activity in which elevated rights are explicitly required.

21.2 Inappropriate use of administrator accounts includes internet browsing, email usage and using common business applications such as Microsoft 365 (i.e., OneDrive, Outlook, SharePoint, PowerPoint, Word, Excel, OneNote, Team). Daily work using common business applications must be performed with standard user accounts.

21.3 Appropriate use of Local Administrator privileges is required to ensure a consistent and manageable set of desktop applications are deployed in a supportable suite size while preventing unsupported tools, only identified and authorized administrators will have the ability to log into workstations performing actions limited to the local administrator role. There will be two types of administrator roles established:

- ➢ Pre-approved roles with standing admin capabilities required to perform core job functions, (e.g. Desktop Support or Solutions Desk personnel in a troubleshooting or end-user service capacity)
- ➢ A set procedure to enable users to request and be granted Local Administrator capabilities on an ad hoc basis to facilitate specific tasks. Ad hoc access permissions will be timebound.

21.4 Privileged access must be granted to a separate account that is used for performing administrative functions. Standard user accounts used for daily business (like email or internet access) may not be granted elevated privileges or used to perform administrative functions.

22. Granting Administrative Access

22.1 Administrative access and account provisioning may be granted only by the Enterprise Services Team based on an established and documented business need. Granting access must follow the procedure outlined in Procedure for Granting Administrative Access to City Information Systems through Service Hub.

- ➢ This includes account provisioning, deprovisioning or adjustments to permission levels.
- ➢ This also includes temporary account permission escalations for just-in-time access, ongoing account permissions management (e.g. server team) and granting of local admin permissions.
- ➢ Temporarily elevated privilege will be limited in scope and credentials “checked-out” for a predetermined, limited timeframe.

- Access must adhere to the principle of Least Privilege as it relates to minimal permission levels required to complete work tasks. Any particular user's or group's access should be documented sufficiently to withstand evidentiary review for audit purposes.
- Individuals must complete training before being granted any kind of administrator account and repeat that training annually to maintain access to those accounts. If the training is not completed each year, the user's admin account will be made unusable until the training is complete.
- Special Considerations for the "Global Administrator" (GA) role:
  - The number of accounts with the permanent Global Administrator role, Privileged Access Manager (PAM), will always be 5 or fewer throughout the enterprise.
  - The Global Administrator account will be cloud only account.
  - The Permanent Global Account that is a non-identifiable and checked out only for major cloud outages ("break glass"); no more than 5 individuals will have access
  - Privileged Identity Management (PIM) eligible (just-in-time) Global Administrator will be cloud only accounts
  - PIM eligible (just-in-time) Role Based Access Management (RBAC) will be federated seattle.gov admin accounts
  - Elevated federated seattle.gov cannot be standard mail-enabled user accounts
  - Local Domain Admin accounts cannot be synchronized
  - All elevated accounts (RBAC/GA) MUST use MFA
  - Temporary Global Admin privileges can be accessed using PIM Privileged Identity Management where privileges will time out after specified time.
  - Permanent Global Administrator accounts will only be used for temporary, emergency, "break glass" forms of troubleshooting or issue resolution and never allocated to a service, an application, or other activities not under the direct and exclusive control of authorized individuals.
  - Central logging and monitoring shall be enabled for all privileged domain and cloud accounts
  - Monitoring and response protocols shall be implemented to respond to all uses of Global Administrator accounts, to confirm legitimate "break glass" use cases
  - Global Administrator accounts should never be used within any standard, anticipated or regular business operations of any City Department or individual except when it is appropriate for an authorized individual to perform emergency ("break glass") remediations and only until those remediations are complete. Any other daily, temporary or ongoing business or administrative tasks will only be performed with less privileged roles than Global Administrator.

22.2 An administrator is associated to an individual and only that individual is authorized to use the administrator account.

22.3 A user with administrator access must obtain a separate ADM account and use that account for Administrator actions. Administrator or elevated rights must not be granted to standard user accounts.

22.4 On-Prem and per Cloud administrative rights must also utilize separate admin accounts

23. Service Accounts

23.1 Service Accounts will be created in support of an application or system and are used to run a service related to the application or system.

23.2 Service Account names should reflect the function of the Service Account and adhere to agreed upon naming conventions.

23.3 Service Accounts must be configured with the least level of privilege required to run the service for the application or system.

23.4 Service Accounts must have an identified and auditable owner to be either an appropriate individual currently associated with the service or a similarly associated team.

23.5 Service Account must be configured so they can't be used for interactive logon

23.6 Non-Service accounts must be prohibited from logon as a service.

23.7 Service Account passwords must adhere to the same length, complexity (including avoidance of passwords on exclusion lists), and history restrictions as user accounts.

23.8 Provided all conditions immediately above are met, Service Accounts passwords may be reset on an annual basis rather than 60 day cycles.

23.9 Service accounts must be actively monitored for inappropriate usage.

Access Control

Access control measures required for establishing Users' access to any City computing resources shall be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved. See GUI101 Access Control and Authentication Guideline for direction on how to assess and define the appropriate security measures for computing systems.

24. Account Management and Authentication

24.1 It is the responsibility of all System Owner/Operators and Data Custodians to ensure that their systems comply with security policies and standards, and the associated System Security Plan and periodically review accounts for compliance with account management requirements.

24.2 Systems are required to have a technical access control mechanism(s) that deploy authentication measures appropriate for data and departmental security requirements. Authentication measures must be commensurate with the required account, data and application security (See Access Control and Authentication Guidelines)

24.3 All systems are required to log basic information about User access activity, system events and errors, and access violation reports.

24.4 All system access accounts for Users must be based on a unique credential that establishes identity based on the City's Active Directory or via federation to that system.

24.5 No shared accounts are allowed except where authorized under the Shared Account Standard or as an exception under the exception process. If a group or shared account is allowed by a policy exception, it must have controls providing an audit trail connecting an individual user to any action performed under the shared credential. All group or shared accounts must reset the shared password when any user leaves the group.

24.6 Applications requiring authentication, whether hosted on premises or in a City or vendor-operated cloud platform, must integrate with the City's Single Sign On (SSO) standard for applications. All new or upgraded applications must authenticate using the City standard authentication platform.

25. Multi-factor authentication

25.1 Multi-factor authentication must be used to ensure positive identification of individuals accessing identified systems or with elevated privilege levels or access to sensitive resources. Examples include:

Standard users authenticating to systems that can only be accessed via MFA;

Administrators of network or database systems or infrastructure;

Contractors accessing internal resources from outside the City network

25.2 Multi-factor authentication may be required for additional use cases, and as further defined in the Multi-Factor Authentication Standard (STA204)

26. Measures

26.1 Automatic Workstation Screen Locking - All City workstations must automatically go into a password-protected screen-lock mode after fifteen (15) minutes of inactivity.

26.2 Unsuccessful logon attempts:

- Locking the account after (6) consecutive invalid logon attempts by a user; and
- Automatically locking the account for 30 minutes or until released by an administrator

26.3 Account Disablement:

- Accounts belonging to separated employees/consultants/volunteers will be terminated within 24 hours unless earlier termination is requested by the Department.
- Inactive accounts will be disabled after 90 days
- Vendor accounts will be disabled at the time of account expiration (default is at end of contract or one year from initiation).
- Note: content to be extracted to *Standard* document

Physical Security

As with logical security measures at the City, physical security measures required for protecting City computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved.

27. Physical Security

27.1 Physical access control measures must be implemented sufficient to prevent City assets from unnecessary and unauthorized access, use, misuse, vandalism, or theft (See GUI105 Physical Security for detailed guidance).

27.2 Certified smoke and fire alarm and fire suppression systems must be in place for larger data centers, server rooms and telecommunication closets and vaults.

27.3 Environmental control measures (power supply, heating, ventilation, air conditioning, plumbing, physical location) must be in place and monitored, tested and maintained regularly.

27.4 Inventory Control measures must be implemented, such as asset tags or other identification markings for tracking and accounting of City assets.

27.5 The City must have secured off-site data/media storage and procedures.

27.6 Specific procedures and security education for all Users of City laptops, wireless services, and other mobile computing devices must be instituted.

27.7 All specific tools, systems, or procedures implemented to meet physical security requirements will be selected on the basis of its ability to meet City specifications and performance requirements and be purchased in compliance to the City's procurement policies and procedures.

Personnel Security Measures

28. Personnel Security Measures

28.1 When hiring employees for key technical positions, comprehensive pre-employment screening must take place.

28.2 All pre-employment inquiries must be conducted in full compliance with all official City and specific departmental policies and in full compliance with all related state and federal laws.

28.3 New employees must be informed about their responsibilities and the policies that apply.

28.4 All employees are required to complete yearly training on the basic tenets of this information security policy.

28.5 All physical and logical access to computing and network facilities and resources must be assigned with the principles of least privilege and separation of duties.

28.6 When terminating employees all City departments must establish processes to quickly close and remove all system and network privileges.

28.7 Related procedures regarding employee suspension, transfers within the city, leave of absence, long term illness or disability must also be established and maintained.

Remote Access

Remote web-based access to certain city systems, applications and data is granted to all City users for the purpose of accessing their email, files, productivity tools and business applications while conducting city business at home, working remotely or traveling (e.g. O365).

Other remote access systems may be restricted only to those employees with an express need and authorization for this type of access. Network support personnel are an example of those that may need remote control capability. Personnel that travel or fill an on-call role are an example of a need for remote access capability.

29. Authorizing and Provisioning

29.1 Those using remote access must be positively identified and authenticated prior to being connected to City of Seattle resources. Multi-Factor Authentication may be required depending on user role, privileges granted, or specific system or network being accessed.

29.2 Remote access sessions must be securely logged with enough attribution to assure identity.

29.3 Passwords must be encrypted during transmission.

29.4 Users are required to use personal firewalls on their computers when accessing the network remotely.

29.5 Unauthorized or self-configured remote access is prohibited.

29.6 City employees must exist in an authoritative directory group indicating authorization for remote access.

29.7 All City of Seattle employees accessing the City network remotely should use the approved methods and technology best suited for the type of work being performed, the network environment and computer resources used. The City provides the following vehicles for remote access, depending on whether the connecting endpoint (remote computer) is City-owned and managed, or personally owned:

- A City-managed system may obtain full VPN access to the network, for access to arbitrary systems within the purview of the individual obtaining the access. Virtual Private Network (VPN) should be used whenever accessing from an unknown or public network location (e.g. library or coffeehouse wi-fi).
- For personally owned systems, remote access must be through a proxied connection, which limits access to only those resources and services for which the individual has an authorized need (e.g. O365 web apps, SharePoint and accessible city applications, VPN as required).
- City documents and data shall be saved to appropriate locations:
  - OneDrive for Business
  - SharePoint
  - Shared File servers via VPN
- City documents and data shall be not saved to unauthorized locations
  - Personal device or personal external hard drive (including smartphones)
  - Unapproved cloud services (e.g. Drop Box, Box, or Google Docs)
  - Removable media shared with personal device (e.g. USB/"thumb" drive)
- Devices that obtain remote access to internal network assets may be scanned for compliance with these policies on a periodic basis by Cybersecurity Operations and/or Information Assurance Team within DSR Division in Seattle IT Department.
- Devices may not extend local administrative rights to the user unless a policy exception has been granted.
- Automatic operating system and critical component updates must be enabled for remote devices.

29.8 Other than the requirement for separate approval before allowing the initiation of remote-control sessions via the VPN, the same policies regarding Acceptable-Use of City technology will apply to remote access as would apply to access originating from City of Seattle internal networks.

29.9 Firewalls must be configured to only allow designated traffic.

30. Contractor Access

Authorized users or contracted vendors must use only authorized methods for remote access to the Network and City services

30.1 Contractors must meet or exceed this policy

Departments granting remote access will ensure that authorized users and contracted vendors sign an Acceptable Use Agreement including a background check when required for accessing data classified as Confidential Requiring Special Handling.

30.2 Contractors accessing internal resources from outside the City network must use multi-factor authentication

31. Vendor Access

Vendors may be allowed remote access to specific servers as needed to provide support to the City of Seattle, subject to the following policies:

31.1 Access into the City of Seattle network will be via the standard VPN solution unless by exception.

31.2 The vendor must sign the City's Acceptable-Use Policy.

31.3 Vendors must have unique user accounts assigned to them for any system that they will be accessing. Vendors are not allowed to operate under the credentials of City of Seattle support staff, or use "shared" vendor accounts.

31.4 City of Seattle support staff must monitor vendor activity at all times the vendor is connected to City resources.

31.5 Vendor remote sessions must be terminated when not actively in use.

32. Coordination of Remote Access Controls for Vendors

32.1 Vendor shall coordinate with City to control vendor-initiated interactive remote access and ensure system-to-system remote access is managed in a manner acceptable to the City. This may include specification of specific IP addresses, ports, and minimum privileges required to perform remote access services. Where technically feasible, vendors shall use individual user accounts with multi-factor authentication that can be configured to limit access and permissions based on the principle of Least Privilege.

32.2 Where the vendor is provided with remote access to City systems, the vendor shall:

32.2.1 1. Maintain their IT assets (hardware, software and firmware) connecting to the City's network with current updates to remediate security vulnerabilities or weaknesses.

32.2.2 2. Document their processes for restricting connections from unauthorized personnel.

32.2.3 3. Ensure vendor personnel do not disclose or share account credentials, passwords, authentication tokens, establish unauthorized connections,

32.2.4 4. Not take any actions while remotely connected to the City's network that are not explicitly authorized.

32.3 For vendor system-to-system connections that may limit City of Seattle's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

33. Remote Control

Refers to the capability of controlling or operating a City of Seattle workstation from another workstation, either inside of or outside of the City of Seattle network.

33.1 Support group personnel may have remote control capabilities to workstations to aid in problem solving. Support group personnel must obtain the approval of the workstation operator before controlling the workstation remotely.

33.2 The remote-control software must notify and obtain approval of the user that is currently logged in before granting access to a workstation. This ensures the end user is aware that someone else is looking at what is on the screen.

33.3 Remote control sessions must be logged to the extent possible. At a minimum, connection attempts should be logged on both success and failure. Remote control logs are to be retained one (1) year.

33.4 Remote Control sessions must automatically disconnect when idle for 15 minutes. The Support group has the authority to make exceptions to extend beyond 15 minutes of idle time when there is a business justification, such as when running scripts, to support the customers of Seattle IT Department.

33.5 Persons controlling workstations remotely must not be allowed to blank the screen or lockout the keyboard or mouse from use by user.

C. SYSTEM AND NETWORK CONFIGURATION

Systems and Network Security

All systems and network security measures must be based on the functional nature and degree of criticality of the computer systems, network resources, and data involved.

34. Systems and Network Security

34.1 It is the responsibility of all System Owner/Operators (see ITSP Appendix: Responsibilities) to ensure that they have implemented all necessary security measures.

34.2 Operating systems must be maintained with the timely application of all related vendor issued patches as described in Patching below.

34.3 Desktop or laptop workstation computers must be deployed following the City standard configuration (see STA113 End User Hardware and Software Standard).

34.4 Each system must maintain a baseline configuration, with settings documented, and exceptions to security controls documented. These must be maintained and monitored through the continuous monitoring strategy

34.5 Where appropriate, systems must have anti-virus software and maintain procedures for regular signature updates (see GUI108 Antivirus Measures).

34.6 Procedures must be maintained for regular backup of all data and system files necessary for recovery purposes (see STA208 Backup, Recovery and Data Retention Standard), with regular restoration testing of critical systems annually at a minimum.

34.7 All systems are required to have the capability to log basic information about User access activity, system changes, and events to enable central collection and monitoring. (see GUI103 Logging Guideline). All systems, applications, and devices must forward relevant security logs and alerts to an approved Security Information and Event Management system.

34.8 All systems must maintain a functioning and accurate system clock.

34.9 All network interconnections to non-City owned systems and all traffic controlled via a managed interface between the City and the external entity shall be explicitly authorized and documented Communications may be monitored for unauthorized or anomalous activity.

34.10 All in-scope computing systems and servers hosted on City IT networks must support proactive vulnerability probing and reporting (see GUI109 Firewalls and Intrusion Detection Security).

34.11 System Owner/Operators (see ITSP Appendix: Responsibilities) must ensure that no function, application, or other computing process is executed on their system(s) that uses an unreasonably large amount of bandwidth on City networks.

34.12 USB connected, serial, or other portable devices are not allowed to be connected to City systems unless and until an exception request stating a legitimate business reason is received and accepted by Digital Security and Risk.

34.13 USB connected, serial, or other portable devices are inherently insecure and thus are discouraged for use as storage for City records, especially sensitive or confidential records (see above).

34.14 Unauthorized, non-City owned and managed network devices (i.e. firewalls, switches, routers, wireless access points) are not allowed to be connected to City systems at any time.

34.15 Any device containing a modem or other external connection and containing an operating system is not allowed to be connected to City systems without a written exception approval from Digital Security and Risk (DSR). Exception requests will not be granted unless these deployments adhere to strict configuration guidelines as outlined in STA-113 End User Hardware and Software.

34.16 No device may be connected to the City's network that does not conform to City standard configuration without expressed approval through an Exception Request.

34.17 System Owner/Operators (see ITSP Appendix: Responsibilities) must display security warning banners prior to allowing the access logon process to be initiated by Users (For an example see GUI112 Use of Security Warning Banner).

34.18 All servers deemed critical to City business functions and/or containing confidential or restricted data must have Host Intrusion Detection/Intrusion Prevention systems installed with alerts routed to a SIEM device (Security Information and Event Management).

34.19 All servers deemed critical to City business functions and/or containing confidential or restricted data must have the capability to implements a set of segmentation controls that are designed to meet both operational and regulatory compliance requirements. (see Network Segmentation and Access Management in the NGDC Architecture).

35. Patch and Vulnerability Management

35.1 Software vulnerabilities will be limited by using secure coding practices and verified via application vulnerability scanning.

35.1.1 Any new code being deployed to production should be free from all "Critical", "High" and "Medium" vulnerabilities before going live. Other items flagged as "Best Practices" will also be implemented before going live.

35.1.2 Application Owners will be responsible for ensuring that all software updates and security updates are applied within a reasonable timeframe following their availability and during the specified maintenance window for the application.

35.1.3 Application Owners are responsible for establishing and managing maintenance windows in coordination with vendor or internal development teams as appropriate.

35.2 All System Owners must institute practices that require all devices have designated security patches applied to system and application software and/or firmware. When required, users will be alerted to reboot their computers to complete security patch deployment within standard designated time frame, after which the computer will automatically reboot with appropriate notification.

35.3 Image files used to configure computing devices must be maintained at current patching levels and should be considered "untrusted images" (see ITSP Appendix: Definition) until scanned for compliance.

35.4 System Owners must be able to provide records of their compliance with this policy within 24 hours of a request by the DSR.

35.5 If system or application software cannot be patched; System Owners must employ and document risk mitigating measures in order to minimize the probability of system compromise until such time as the software can be patched.

35.6 Decisions as to criticality will rest with the DSR in consultation with System Owners where necessary.

35.7 When a need for security Patches of significant severity are identified outside of normal cadence, notice will be disseminated by the DSR via email to identified contact persons for each affected System within the next patch window.

35.8 A contract for any new City system designed and/or deployed in collaboration with, or exclusively by, outside vendors shall include specific language clearly identifying the party to be responsible for patching and maintenance of that system and its attendant applications.

35.9 Vendor contracts will identify specific remedies for any damages caused by failure to maintain the system or its associated applications and will also identify the party responsible for incident response and repairs.

35.10 Any software installed by users with elevated rights must be regularly patched and maintained in accordance with the Patch Management Standard.

35.11 Virtual Patching capabilities may be leveraged as compensating controls where approved by DSR.

35.12 Exceptions to this policy may be granted as necessary.

35.13 All QA and production environment servers will be configured to meet hardening standards and updated on a monthly cadence, or one that more closely aligns to vendor release schedules, to incorporate the latest software updates and security patches. New servers in those environments will be created using only the latest configuration and patching levels to avoid the introduction of any known vulnerabilities. Server operating systems no longer receiving support packages must be upgraded or removed from production environments prior to that end of support date unless there is a system security plan with appropriate compensating controls that has been pre-approved by DSR.

36. Virus/Malware Protection

36.1 Anti-malware software will be purchased and installed for all LAN, application and database servers and workstations.

36.2 Antivirus software must be updated on a regular basis. Servers and workstations must be scanned periodically, either manually or via an automated program.

36.3 Servers that store, process or transmit restricted or confidential data (See GUI110 Data Classification Guideline for data classification descriptions) in any form must be protected by a host-based intrusion detection system (HIDS) (See ITSP Appendix: Definition).

36.4 System Owners must report all suspected or confirmed virus or malware incidents to the Service Hub either manually or via automated tool.

36.5 In the event of a serious virus outbreak, or threat to the City's network caused by malware, a computer or department may be disconnected from the network.

36.6 A virus outbreak or other threat to the City's network will result in the initiation of the Cyber Incident Response Plan.

37. Wireless Access

37.1 Wireless technology is inherently insecure (see ITSP Appendix: Definition) - for specific examples of wireless technology). No wireless deployments are allowed unless a written business case has been received and reviewed and an exception to this policy is approved by the DSR.

37.2 In-scope devices with enabled wireless capability will ensure that authorized users and contracted vendors sign a Vendor Acceptable Use Agreement.

37.3 Departments deploying devices with enabled wireless capability for general use will ensure that an Acceptable Use Agreement is signed by the administrators of those devices.

37.4 System owners and/or operators must terminate and remove wireless enabled computing devices within one business day of notification that an authorized user or contracted vendors' privileges have been revoked.

37.5 Authorized users who access City restricted sensitive or confidential data must be authenticated through access mechanisms as outlined in the Access Controls Policy.

37.6 Devices must be approved and authorized before establishing a local or remote connection to the City IT network.

37.7 Authorized users and contracted vendors are accountable for all activities while connected via wireless enabled computing devices and will be held accountable should the access privilege be misused.

37.8 Wireless devices must be deployed with a software or hardware host firewall application or device.

37.9 Data classified as sensitive or confidential must be protected in accordance with City Procedures (see GUI110 Data Classification Guideline).

37.10 All City owned and managed wireless networks connected to the City backbone will be so identified with a welcome banner as referenced in GUI112 Use of Security Warning Banner.

37.11 Dual homing is not allowed, so wireless devices must be setup with separate profiles for wireless and wired connections.

37.12 Wireless devices and network must employ the same logging and monitoring capabilities as wired devices.~~.~~

Risk Management

38. Risk Management and Security Assessment

Information security programs must be driven by a clear and current risk management strategy. This responsibility is Citywide and must be addressed in programs which include collaboration and cooperation by all City departments, and with full executive level support.

38.1 A continuous risk assessment will be carried out with management from the DSR that identifies threats, vulnerabilities, and results in a formal risk assessment. The risk assessment will include a gap analysis and mitigation plan. This assessment should include an externally performed penetration test or red team exercise.

38.2 Department specific assessments will be completed, as appropriate, focusing on critical IT systems and services.

38.3 Maintain a security controls matrix and update on a regular basis, using industry best practices from Center for Internet Security (CIS) controls and NIST 800-53 controls.

38.4 System Security Plans shall be maintained for all systems, and approved by DSR. Whenever possible, systems will use City standard benchmarks and the City's security controls to determine as their baseline security settings and configurations. Any exceptions to these will be documented in the system security plan.

38.5 A plan of action and milestones (POAM) shall be maintained to track implementation of security controls to various systems, as defined in the approved system security plans and security controls matrix.

38.6 The City will maintain a cybersecurity risk register to be reviewed and presented to security governance groups annually, at a minimum.

38.7 The City will implement and maintain a continuous monitoring strategy to track risk approach, POAM accomplishment, and security controls compliance.

38.8 Each system must maintain a baseline configuration, with settings documented, and exceptions to security controls documented. These must be maintained and monitored through the continuous monitoring strategy.

39. Asset Lifecycle Policy

Seattle IT is committed to managing the lifecycle of its IT assets. Employees have a duty of care to protect IT assets at all times whether they are in use, storage, movement, or in disposal.

- ➢ IT assets shall be protected against physical or financial loss whether by theft, mishandling or accidental damage either through primary prevention (e.g. physical security) or remediation (e.g. marking).
- ➢ All IT assets shall be traceable and auditable throughout the entire lifecycle.

40. Inventory of IT Assets

40.1 Seattle IT shall maintain an inventory of IT assets which consist of physical IT assets (e.g., system, network devices and peripherals), logical IT assets (e.g., licensed software, data stores, and, cloud computing licensing) and all components within the authorization boundary of the City's information systems.

40.2 Seattle IT Divisions must also identify ownership of IT assets and must collect the appropriate information for each asset which they own and/or are responsible for.

40.3 Asset Management will maintain a list of Seattle IT's official Inventories. DSR will have access to view the list as required for security purposes.

40.4 All organizations deploying or maintaining compute systems or related items shall be responsible for ensuring their operating inventories are listed in the officially recognized list of city compute inventories. DSR will be provided the inventory location and read only access.

41. Safeguarding IT Assets

41.1 All assets will be recorded and maintained in approved registers by the Seattle IT. To manage the registers accurately and efficiently, all employees shall adhere to the following:

41.2 City of Seattle users shall not remove IT assets supplied by the City from the City's premises, unless approved by exception in advance.

41.3 City of Seattle employees may not connect personal IT assets to the City's private network and data (Connection to provided "Guest" or "Public Access" networks is allowed).

42. Disposal of IT Assets

42.1 Disposal of Seattle IT assets, including the sale, transfer, donation, or sustainable disposal (recycling), must be done in adherence with all federal, state and local regulations and in accordance with data classification and handling requirements relevant to industry regulatory requirements (e.g. PCI, NERC, CJIS). Computer hardware must have all software and information securely removed prior to disposal where practicable or be destroyed through approved means.

D. DATA MANAGEMENT

Data Management

Access to City data will be made possible consistent with the classification of the data, business need, user role and privilege level.

43. Data Classification

43.1 Data will be classified according to its sensitivity to unauthorized exposure as defined per the Data Classification Standard. The classification level applied to specific information is based on statutory requirements, the sensitivity of the data, its criticality to the City, and its use. For classification guidelines and best practices (see GUI110 Data Classification Guideline).

43.2 All data defined as highly sensitive by industry or governmental regulatory groups will be classified at the highest level (as Confidential Information Requiring Special Handling).

43.3 Data classified as Confidential Information Requiring Special Handling will be managed in accordance with their requirements. Separate specific policies or standards may further define specific handling requirements including specifications for handling, inventory, labeling, back-up verification, disposal, specific transmission and storage specifications.

43.4 Data in restricted/protected classifications must be encrypted as appropriate to its sensitivity and regulatory requirements.

44. Electronic Data and Records Management

44.1 All City System Owner/Operators, Data Custodians, and Users (see - Definitions), are obligated to understand the nature and proper classification of the data they generate, use, or store.

44.2 All City System Owner/Operators, Data Custodians, and Users, are required to properly manage and protect the confidentiality of private or sensitive electronic data they may be using, transmitting, and storing. For classification guidelines and best practices see GUI110 Data Classification Guideline.

44.3 All City System Owner/Operators, Data Custodians, and Users are required to understand and comply with all records retention laws for any electronic data they may be using, transmitting, and storing.

44.4 NOTE: Be aware that the City Records Management Program (CRMP) maintains specific records management information and offers consultation to users and management on their retention obligations under State law.

45. Data Sharing

45.1 The City of Seattle facilitates information sharing with partner entities by enabling authorized Department leadership to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for particular data classification and regulatory requirements.

- ➢ Partner may be defined at the individual, group, or organizational level.
- ➢ Information may be defined by content, type, security category, special access requirements or restrictions.

45.2 The organization employs defined mechanisms, processes and documentation to assist users in making information sharing collaboration decisions.

46. Electronic Data Breach Disclosure

46.1 A "reportable security breach" is defined by Washington State and Federal law.

46.2 The City of Seattle will comply with all applicable laws. See Cyber Security Incident Management Plan for details of the procedure to follow if a breach is suspected.

47. Rules Specific to Electronic Communication Usage

47.1 Electronic communication (e-mail, IM, IRC, SMS) is a temporary medium and, therefore, inappropriate for substantive policy messages

47.2 Electronic communications that contain substantive policy messages must be archived per email management rules and guidelines in appropriate retention folders.

47.3 Individual users may use approved methods for screening their e-mail to screen unwanted e-mail from, or to automate filing of, their individual accounts.

47.4 Electronic communications sent to members of the public must be consistent with the City's published Privacy Policy and this Information Technology Security Policy, including ensuring:

- The intended recipient specifically request to receive the communication from the City
- Ensuring the proper protection of personally identifiable information (i.e.,PII such as a person’s e-mail address)

47.5 City departments and vendors acting on behalf of the City will not send unsolicited emails to constituents or City employees over the public Internet that ask them to reply with confidential information or that that ask them to click on embedded links to City web self-service transactions that require entry of confidential information.

47.6 Any City department providing public Internet self-service transactions that collect confidential information is required to put a notice of the policy as noted in #4 above, and warnings of prevalent spoofing and phishing methods; or a link to such a notice, on web pages that describe or contain the self-service transactions.

47.7 Any City department that provides public Internet self-service transactions that collect confidential information shall periodically provide notices of City policies and warnings of prevalent spoofing and phishing methods in regular constituent correspondence.

47.8 Any outgoing messages which do not reflect the official position of the City of Seattle or the user's department must include the following disclaimer: "The opinions expressed here are my own and do not necessarily represent those of the City of Seattle."

47.9 All general distribution messages must contain the name of the approving authority (departmental e-mail administrator or designee) and the date of approval. All requests for citywide broadcasting must be sent to the email Administrator e-mail account.

47.10 Departments must implement department level guidance, where appropriate, regarding the departmental use of electronic communications.

47.11 Each department shall identify a Departmental e-mail administrator who will enforce and monitor this policy.

47.12 Only City standard applications may be used for any type of electronic communications, including e-mail and Instant Messaging (IM) unless a business need has been documented and an exception granted by Seattle IT Department.

47.13 Standard configurations must be conformed to for all electronic communications systems (See the STA-104 Bulk Email and SMS Communication)

47.14 Instant Message systems specifically are not allowed to accept inbound attachments or links and must only use the user's seattle.gov email address as an identifier.

47.15 All Users are required to understand and comply with all records retention laws for any electronic communications they transmit, store or disseminate

Encryption

The need for encryption of information is based on its classification, risk assessment results, and use case.

Attention must be given to the regulations and national restrictions (e.g., export controls) that may apply to the use of cryptographic techniques in different parts of the world. The U.S. Government restricts the export, disclosure, or release of encryption technologies to foreign countries or foreign nationals, including “deemed exports” to foreign nationals within the United States (excluding those foreign nationals with permanent resident visas (i.e., Green Cards), U.S. citizenship, or ‘protected person’ status). If you have any questions, please contact Counsel and Legal Services.

Encryption products for confidentiality of data at rest and data in transit must incorporate Federal Information Processing Standard (FIPS) approved algorithms for data encryption.

48. Encryption in Transit

Encryption is required for data in transit in the following situations:

- When electronic personally identifying information (PII) is transmitted (including, but not limited to, e-mail, File Transfer Protocol (FTP), instant messaging, e-fax, Voice Over Internet Protocol (VoIP), etc.).
- When data is classified “Confidential” or higher
- When encryption of data in transit is prescribed by law or regulation.
- When connecting to the internal network(s) over a wireless network.
- When remotely accessing the City’s internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, infrared) network. This does not apply to remote access over the City’s managed point to point dedicated connection.
- When data is being transmitted with one of the City’s public facing website and/or web services, they are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP) where technically feasible. Public facing websites must utilize HTTP Strict Transport Security (HSTS), automatically redirecting HTTP requests to HTTPS websites where technically feasible.

49. Encryption at Rest

Encryption is required for data at rest, including in the following scenarios:

- For the systems listed below:
  - Desktops that access or contain personally identifying information (PII);

  - Data stores (including, but not limited to, databases, file shares) that contain PII;
  - When data is classified "Confidential" or higher
  - All mobile devices, whether City issued or third-party, that access or contain any City information; and
  - All portable storage devices containing any City information.
- When electronic PII is transported or stored outside of the City of Seattle facility.

Appropriate encryption methods for data in transit must employ current unbroken algorithms; these include, but are not limited to, Transport Layer Security (TLS) 1.2 or later, Secure Shell (SSH) 2.0 or later, Wi-Fi Protected Access (WPA) version 2 or later (with WiFi Protected Setup disabled) and encrypted Virtual Private Networks (VPNs). Components should be configured to support the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled.

Compliance

Applicability

If implementing a new technology (solutions, systems, software, hardware and networks), that technology may not go live unless in compliance with this Policy. Existing (legacy) technology must implement this Policy as part of any major upgrade.

Measurement

Adherence to these provisions will be periodically assessed by leadership as well as through audits conducted in specific focus areas.

Exceptions

Exceptions must be approved in advance through submission of a Seattle IT Security Policy Exception request in Service Hub. This can be submitted directly or with assistance of Client Engagement personnel.

Non-compliance

The Chief Technology Officer (CTO) is responsible for compliance of this policy. Enforcement may be imposed in coordination with individual division directors and department leaders. Non-compliance may result in disciplinary action, restriction of access, or more severe penalties up to and including termination of employment or vendor contract.

Related Standards and Policies

See ITSP X – Appendix Related Documents

Responsibilities

See ITSP X – Roles

Definitions

See ITSP X – Definitions

Authority

SMC 3.23.030 (section C & D) assigns responsibility for the administration of the development of policies and standards for governing the acquisition, management, and disposition of information technology resources and the management, maintenance and operation of City information technology resources to the Chief Technology Officer

Document Control

This policy shall be effective on 12/31/2020 and shall be reviewed at least annually. The next review shall occur by 12/15/2021

Version	Content	Contributors	Approval Date
v 1.0	Initial Draft	Consolidated Update: Keith Cooke Reviewer: Andrew Cushman - CISO	**10/25/2019**
V 1.1	Revision/Updates	Keith Cooke, DSR Compliance and Risk teams Consultation and Review with various ITD SMEs	**5/19/2020**
	Policy and Standard Review Board	Ben Featheringill, Bob Keenan, Chris Wood, Daniel Ward, James Sprinkle, Jeff Brausieck, Jeffrey Roy, John Alton, John Engstrom, John Jacobson, Jonathan Porat, Kelly Eden, Keri Jones, Kristi Mauck, Kristina Pham, Max McGrath, Paul Haase, Ron Co, Sarah Carrier, Stephen Beimborn, Vinh Tang	**5/18/2020**
	Final	Approver: Andrew Cushman - CISO Saad Bashir - CTO	**5/26/2020**
V 1.2	Update for Local Administrator and Compliance Activities	Reviewed: SME, Policy Standard Advisory Board Approver: Saad Bashir - CTO	**12/30/2020**
V 1.3	Updates to Access Control and Data Management sections	Reviewed: SME, Policy Standard Advisory Board Approver: Saad Bashir - CTO	**6/30/2021**
V 1.4	Updated Guidelines and Library Links	Reviewed: CISO IT Policy Review Approver: Jim Loter - CTO	**12/30/2022**

Jim Loter (Dec 22, 2022 08:25 PST)