BTS-2.01 - Information Security Administrative Rule

Administrative Rules Adopted by Bureaus Pursuant to Rule Making Authority (ARB)

Policy category: Information Security

Policy number: BTS-2.01

Subsection 1 – General Administrative Rule

Purpose

The purpose of the Bureau of Technology Services (BTS) Information Security Administrative Rule is to ensure the security and availability of City Technology Resources, including systems, assets, networks and information. The BTS Information Security Administrative Rule also helps ensure confidentiality, integrity and availability of electronic information captured, maintained and used by the City of Portland. This policy shall be used as a foundation for all Citywide policies, standards, procedures, and guidelines that are developed and implemented by the City, related to information security and compliance. As of 2023 the BTS-2.xx Information Security Administrative Rules have been consolidated into this one policy.

The Information Security Administrative Rule is a "living" document that will be altered as required to address changes in technology, applications, procedures, legal and social imperatives and potential cyber threats. Please reach out to the Information Security team with any needs, questions, or concerns: *BTS - Information Security* *btsinfosec@portlandoregon.gov*

The BTS Information Security Administrative Rule is technical in nature, combining technologies, resources, processes, applications, and workforce compliance to policy expectations as well as legal requirements.

The following Information Security reference documents will aid in applying the BTS Information Security Administration Rule into practice, as securing City information is an integral responsibility for all Authorized Users.

City of Portland Security Standards 4.0 739.21 KB

1. BTS Technology Standards Directory
2. List of Sensitive Information Fields
3. HRAR 4.08 Information Technologies
4. HRAR 1.03 Public Records Information, Access and Retention
5. HRAR 11.04 Protection of Restricted and Confidential Information
6. Glossary | CSRC (nist.gov) – Technology and Information Security terms and definitions

Search Code, Charter, Policy

Keywords

Search

Authorized Users (employees, contractors, vendors, volunteers, and other authorized parties) are responsible for complying with this policy. Unauthorized access to, use, or abuse of City Technology Resources, information and data, including legally privileged information is expressly prohibited. City Confidential, Restricted and Unrestricted (Public) Information classifications are detailed in **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING.**

Authority and Compliance

The Chief Technology Officer (CTO) shall establish and provide authority and governance for information security policies, standards, and best practices for Citywide technology to secure all City Technology Resources, information and data and promote the most efficient use of City Technology Resources.

The Senior Information Security Officer (SISO) is responsible for developing and enforcing policies and standards for the implementation and use of information technology security standards and compliance on a Citywide basis.

The City of Portland is a public entity. The City has custodial responsibilities for a significant and diverse amount of sensitive and confidential information, as referenced above. The City holds business contracts with a broad range of public and private organizations. The City is the recipient of federal and private grants. The City owns, maintains and operates significant critical infrastructures and services including those of public health and safety. These and related responsibilities place significant obligation on the City regarding the management and use of its extensive Technology Resources. Not least among these obligations are compliance requirements with many State and Federal laws, regulations, and promulgated rules. Pursuant to Federal and State regulations, management control of access to law enforcement data, specifically Criminal Justice Information Services (CJIS), National Crime Information Center (NCIC 2000) and Law Enforcement Data Systems (LEDS), are under the authority of the Chief of Police of the Portland Police Bureau. The Bureau of Emergency Communications (BOEC) maintains a separate CJIS role and parallel responsibilities.

Beyond strict compliance requirements, the City must also understand and consider several additional government and industry standards and best practices that contribute to the objective of “due care”.

In addition to the City’s information security governance and compliance requirements, this policy also reflects the City’s strong commitment to its own institutional ethics and values.

Successful compliance and protection of City Technology Resources, assets, information and data requires all Business System Owners, System Operators, Data Custodians and Authorized Users of City-owned technologies, to learn, understand, and support the City's information security policies and associated standards, best practices and guidelines.

Administrative Rule

The Information Security Administrative Rule includes subsections for policies covering the following areas:

Subsection 1: GENERAL ADMINISTRATIVE RULE

Subsection 2: ROLES AND RESPONSIBILITIES

Subsection 3: NETWORK ACCESS AND ACCOUNTS

Subsection 4: REMOTE NETWORK ACCESS

Subsection 5: IDENTITY AND ACCESS MANAGEMENT

Subsection 6: DATABASE PASSWORDS

Subsection 7: PATCHING, MALWARE PREVENTION AND RECOVERY

Subsection 8: INCIDENT REPORTING AND RESPONSE

Subsection 9: MOBILE DEVICES AND REMOVABLE MEDIA

Subsection 10: WIRELESS NETWORKS

Subsection 11: ANALOG MODEMS

Subsection 12: PHYSICAL SECURITY AND ASSETS

Subsection 13: INTRUSION PREVENTION AND DETECTION

Subsection 14: SECURITY ASSESSMENTS, AUDITS, AND PENETRATION TESTS

Subsection 15: ENCRYPTION

Subsection 16: FIREWALL AND SECURITY SYSTEMS

Subsection 17: PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

Subsection 18: INFORMATION CLASSIFICATION, PROTECTION AND SHARING

Subsection 19: CLOUD SERVICES

Subsection 20: SOFTWARE, SYSTEM AND SECURITY DEVELOPMENT LIFECYCLE

In addition to the above policies, the following general information security policies apply to all Authorized Users of the City's technology resources and information:

1. **Altering Authorized Access:** Authorized Users are prohibited from changing access controls to allow themselves or others to perform

actions outside their authorized privileges and assigned responsibilities.

2. **Applicability:** This BTS Information Security Administrative Rule is applicable to all Business System Owners, System Operators, Data Custodians, and Authorized Users of City Technology Resources, associated information or any other electronic processing or communications related Technology Resources or services—including removable media, internet-based and mobile devices.
3. **Authorized User Accountability:** Authorized Users are accountable for their actions in use of City Technology Resources and information and may be held liable to administrative or criminal sanctions for any unauthorized actions found to be intentional, malicious or negligent.
4. **Background Checks:** Background checks may be a requirement for any Authorized User who will be working with or around City Confidential or restricted technology equipment or information. Such determination will be at the discretion of the CTO, SISO, and Business System Owner unless it is mandated by law or State/Federal requirement.
5. **Denial of Service Actions:** Authorized Users are not allowed to prevent Authorized Users or other systems and technology services from performing authorized functions by actions that deny access or the ability to communicate. These include actions that deliberately suppress communications or generate frivolous or unauthorized network activity or service interference.
6. **Electronic Data and Records Management:** The City generates, processes and stores many forms of information. Records Retention and disposition requirements are maintained by and can be found at the City of Portland Auditor's Office.
    a. All City Business System Owners, Data Custodians, and Authorized Users are obligated to understand the nature of the information and data they generate, use, transmit or store—regardless of location or storage medium--and ensure that they are managing that information and data in full compliance with City records management and information security policies.
7. **Exceptions**: Exceptions to this policy must be approved by the CTO or the SISO. In each case, the bureau must request the exception waiver, in writing, and include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the approval from the bureau director requesting the exception.
8. **Information Protection:** Authorized Users are required to protect the confidentiality, integrity and availability of City Confidential or Restricted Information they use, transmit and store. Examples of confidential or sensitive information include but are not limited to; criminal justice data, pending litigation records, employee personnel records, health benefits information and medical files, payment card numbers, in-process procurement evaluation and contract negotiation materials, driver license numbers, social security

numbers, dates of birth, intellectual property and all other information expressly exempt from Oregon public records laws.

    a. A List of Sensitive Information Fields is available for guidance in determining confidential data fields and types.

9. **Malicious Software (Malware):** Authorized Users must not willingly or through an act of negligence, introduce or use malware such as computer viruses, Trojan horses, worms or spyware.
10. **Monitoring of User Accounts, Files and Access:** Related Administrative Rules governing Authorized User use of City technology resources and expectation of privacy, monitoring of use, site blocking, prohibited use, email (including all-employee broadcast email, Union use of email, Netiquette, and email records retention), and malware protection are included in the Bureau of Human Resources Administrative Rules. (In particular: HRAR 4.08 Information Technologies)
11. **Reconstruction of Information or Software:** Authorized Users are not allowed to reconstruct or duplicate information or software for which they are not authorized.
12. **Software Licenses:** All software used on City devices, or hosted by an internet-based service provider, must be appropriately and legally acquired and used according to a City procurement approved licensing agreement. Possession or use of illegal copies of software or data is expressly prohibited.
13. **Tampering with Information Security Software and Settings:** Authorized Users must not tamper with or disable information security software or settings, including but not limited to network password mechanisms, system logs, virus protection software, security auditing and asset management tools, system clocks and software distributions tools.
14. **Unauthorized Access:** Any attempted or unauthorized access, use, or modification of City Technology Resources is prohibited. Unauthorized users may face criminal or civil penalties. Access to or use of City technology resources by any person whether authorized or unauthorized, constitutes consent to City of Portland Administrative Rules.
    a. Authorized Users and unauthorized users are not to access or attempt to access systems, networks or information for which they are not authorized, nor provide access to unauthorized users. Authorized Users are not to attempt to receive non-City business information or access information by unauthorized means, such as impersonating another system, user or person, misuse of Authorized User credentials (user I.D.s, passwords, etc.) or by causing any technology component to function incorrectly. Authorized Users and unauthorized users are not to possess, intercept or transfer information or communications for which they are not authorized.
15. Least Permissions, Least Privilege and Least Function: Systems, accounts and assets must be configured to provide the least permission, privilege, and function required to complete a task.

Unnecessary permissions, privileges, or function must not be assigned to any assets.

16. **Unauthorized Data Alteration:** Entering information into a computer or database that is known to be false and/or unauthorized, or altering a database, document, or computer disk with false and/or unauthorized information is prohibited.

Subsection 2 – Roles and Responsibilities

Purpose

Responsibility for protecting City Technology Resources, including systems, assets, and information, is shared by many entities and individuals throughout the City including the Senior Information Security Officer, Authorized Users, Business System Owners, Data Custodians, and System Operators.

The purpose of this policy is to describe the specific roles and responsibilities of each of these groups and individuals regarding Information Security.

Role and Responsibilities

Senior Information Security Officer (SISO) and Information Security

The Senior Information Security Officer provides a key role of centralized oversight and enforcement for technology systems' security-related services for the City. These responsibilities include, but are not limited to the following key areas:

1. Security policy development, implementation, and enforcement; including granting exceptions to any BTS Security Administrative Rule.
2. Strategic security planning and plan implementation.
3. Security awareness and education programs.
4. Maintain relationships with external entities for threat intelligence and information gathering.
5. Risk Management Strategy, including risk outcomes that identify options to accept, mitigate, deny, and transfer identified risks.
6. Disaster Recovery, Continuity of Operations and Contingency planning.
7. Address Supply Chain and Procurement risks.
8. Risk assessments and incident prevention.
9. Security audits, and penetration tests.
10. Contract review of technology acquisitions.
11. Incident Response services, ensuring the Incident Response Plan is followed and incidents are coordinated with other agencies and entities.
12. Vulnerability management program. An automated and adaptive vulnerability capability for scanning City networks and assets to detect vulnerable and exploitable systems and to identify gaps in patching

and security. See **Subsection 7 - PATCHING, MALWARE PREVENTION AND RECOVERY.**

13. Security consulting services as needed.
14. Development and implementation of all appropriate security standards and guidelines as necessary for the City.
15. Consider impacts to Privacy for each technology under the SISO's purview.

Authorized Users

All Authorized Users have a critical role in the effort to protect and maintain City technology systems and data. Authorized Users, including users who are contractors or 3rd party service providers, of City Technology Resources and data have the following responsibilities:

1. Support compliance with all federal and state statutes and regulations.
2. Comply with all City and Bureau Administrative Rules, policies and guidelines.
3. Protect all City technology assets and information and never share access, accounts, privileges and associated passwords.
4. Always maintain the confidentiality of sensitive information for all uses.
5. See: List of Sensitive Information Fields for guidance in determining confidential information.
6. Accept accountability for all activities associated with the use of their Authorized User accounts and related access privileges.
7. Ensure that use of City and personal technology devices, email, internet access, computer accounts, networks, and information stored or used on any of these systems is restricted to authorized purposes and defined acceptable use policies.
8. Report all suspected security and/or policy violations to an appropriate authority, including your manager, the SISO and BTS Helpdesk.
9. Follow all relevant policies, guidelines and procedures established by City bureaus and offices as well as agencies with which they are associated and that have provided them with access privileges.
10. Comply with all software licensing terms, rules and restrictions.
11. Accounts will be activated, terminated, suspended and managed according to all other relevant policies and procedures.

Business System Owners

Business System Owners play a critical role in the protection of City information systems and data. Business System Owners have responsibility for their managed systems and internet-based services and storage and must:

1. Ensure compliance with all City and Bureau Administrative Rules, policies, standards and guidelines as well as all statutory and regulatory requirements.

2. Segment and protect data into production, development, and test environments.
3. Define the criticality of assets and the level of security required for protection. This is determined by performing a business impact analysis of the critical functions as determined within the asset criticality guidelines and aligned with **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING.**
4. Assign and provide necessary support and authority to appropriate Authorized Users to carry out the functions of Data Custodian(s)* for all managed technology systems and services. Work in cooperation with other Business System Owners for shared systems to ensure that Data Custodian responsibilities are properly fulfilled.
5. Map data flows in a network diagram or network drawing
6. Ensure the confidentiality of sensitive proprietary data especially personally identifiable information, protected criminal justice information, and sensitive information related to protection of critical infrastructure.
7. See: List of Sensitive Information Fields for guidance in determining Confidential Information.
8. Ensure that access granted to Authorized Users is based on the “Principle of Least Privilege” and “Principle of Separation of Duties” as appropriate and where required.
9. Ensure that all incidents of security breaches are documented and reported to BTS HelpDesk and Information Security services personnel.
10. Document and submit any desired exceptions to Citywide policy for review to the CTO.
11. Use Change Control standards and procedures to document, schedule and coordinate maintenance and repair including outages and their resolution.
12. Support all incident response activities that involve respective managed system(s) and services.
13. Advocate for security resources as required in City budget processes and in grant proposals.
14. Define the business parameters for disaster recovery plans, including both the required recovery time objectives and the required information recovery point.
15. Ensure all new Authorized Users are provided with City policies, standards and guidelines.
16. Provide timely notification to BTS, System Operators and Data Custodians in events where access to City technology systems and services is no longer required. Such events include employment termination or job duty change.

Data Custodians (Information Custodians)

The role of Data Custodians is to provide direct authority and control over the management and use of specific information or data. The Data Custodians may be a supervisor, manager, or designated professional staff, assigned the responsibility by the Business System Owners (Bureau Director). They may serve dual roles as a Business System Owners/Operators as well as a Data Custodians; however, this practice must be limited and consistent with the principle of separation of duties, such that they typically would not be the technicians (system administrators) that support the related technology systems, services or applications. Their responsibilities include but are not limited to:

1. Ensure compliance with all Citywide and Bureau Administrative Rules, policies and all statutory and regulatory requirements.
2. Provide System Operators and internet-based service providers the requirements for all access control measures related to the data they are charged with managing and protecting.
3. Support access control to data by acting as a single control point for all access authorization. Maintain data access authorization audit logs and documentation. These audit logs and documents must be reviewed with the System Operators or internet-based service provider.
4. Support regular review and control procedures to ensure that all Authorized Users and associated access privileges are current, accurate and appropriate.
5. Ensure that access granted to Authorized Users is based on the “Principle of Least Privilege” and “Principle of Separation of Duties” as appropriate and where required.
6. Ensure that data backup and retention requirements are aligned with business needs and public records Administrative Rules maintained by the City of Portland Auditor's Office.
7. Notifies the appropriate System Operators or internet-based service provider when access granted to Authorized Users is no longer required.
8. Data Custodians must work in conjunction with System Operators, or internet-based service provider, and Information Security personnel to ensure that “due care” is taken to properly protect City Confidential Information.

System Operators, System Administrators and 3rd party Service Providers

The role of System Operators and internet-based service providers is to provide day-to-day operation of a technology system or service. System operators and internet-based service providers, also referred to as system or service administrators, have the following responsibilities:

1. Works with the bureau (Business System Owners and Data Custodians) to understand specific security requirements as they relate to business criticality, confidentiality and regulatory compliance.
2. Works with bureau (Business System Owners and Data Custodians) to identify appropriate user access to the system and data.
3. Maintains the confidentiality, integrity and availability of City Technology Resources with ongoing patching, monitoring, alerting and

status reports.

4. Works with Information Security personnel to effectively implement technologies and configurations which comply with information security policies, standards, guidelines and procedures.
5. Establishes, prior to implementation, appropriate account access security, technical support access, as well as backup and emergency support.
6. Ensures, as appropriate, that physical and logical access security is always controlled, and that robust backup and recovery mechanisms are employed.
7. Regularly monitors for unauthorized access as well as maintains a history file for auditing purposes and reports any unauthorized or suspicious activity immediately to Information Security personnel.
8. Works with the bureau (Business System Owners and Data Custodians) in preparing disaster recovery plans.
9. Works with the Data Custodians to define proper data backups and with the City of Portland Auditor's Office retention schedules and ensures data and information is consistently maintained in accordance with such schedules.
10. Removes access to City technology systems and Internet-based services immediately upon notification of authorized access change events such as employee termination or reassignment of job duties.

Subsection 3 – Network Access and Accounts

Purpose

Access to City Technology Resources on City networks and within authorized Internet-based Service Provider (hosted services) is essential for many City Authorized Users to do their jobs. At the same time, security considerations require that access is limited to only those persons whose responsibilities require access, and to only those resources required to fulfill their duties.

Remote Access to City Technology Resources requires enhanced Authorized User identification through Multi-Factor Authentication (MFA). See Bureau of Technology Services **Subsection 4 - REMOTE NETWORK ACCESS** and **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING**for requirements.

The purpose of the Network Access policy is to establish rules for Authorized User access and remote use of the City's Technology Resources.

Administrative Rule

1. Access to the City's Technology Resources will be made available to all Bureaus, offices and locations and follow a standard process to determine access requirements for Authorized Users:
    a. City personnel

    b. Volunteers
    c. Community members
    d. Business partners, and
    e. Contracted support personnel
2. Authorized Users will be given access to only those specific resources required to accomplish their job as determined by Business System Owners and Data Custodians.
3. Non-City Authorized Users will not be given access to the City's Technology Resources, except on a case-by-case basis at the discretion of the CTO or by Council action (e.g. Intergovernmental Agreements). Any non-City Authorized User receiving permission to access the City's Technology Resources must abide by all City and BTS technology Administrative Rules, standards and procedures.
4. Security-warning banners must be displayed prior to allowing the logon process to be initiated by Authorized Users. This security banner must inform all Authorized Users that the City Technology Resources being accessed are proprietary, must only be accessed by Authorized Users, and that City Technology Resource usage is monitored for City policy enforcement purposes.
5. Automated changes to access rights must be enabled wherever available.

Responsibilities

Bureau Responsibilities

1. Business System Owners and Data Custodians must identify those Authorized Users who require access to City Technology Resources, including specific network resources and applications. These approved authorizations must be in writing and come from the bureau director or an authorized delegate and maintained by BTS.
2. Business System Owners and Data Custodians must identify the minimum required account access required for an Authorized User to effectively fulfill their responsibilities.
3. For non-City Authorized Users, the responsible Business System Owners or authorized bureau service delivery manager must identify City Technology Resources access requirements with proper written justification and receive prior approval from the CTO or the SISO. Requests for such access can be made by completing the appropriate request form: Account Management | The City of Portland, Oregon (portlandoregon.gov)
4. Business System Owners and Data Custodians or a designated Bureau of Human Resources representative, are responsible for immediately notifying the BTS Helpdesk when access to City Technology Resources should be discontinued. An example includes termination of employment or assignment to responsibilities and duties for which access is no longer required.
5. Data Custodians, or those who manage bureau specific data which can be accessed by multiple Authorized Users, are responsible to conduct bi-annual audits to ensure assigned Authorized Users

continue to require access. Any required changes of access rights must be immediately reported to the Bureau of Technology Services' HelpDesk: BTS Technology Portal.

Bureau of Technology Services Responsibilities

1. Create and delete Authorized User accounts, grant and revoke access to appropriate City Technology Resources as defined by the Business System Owners and Data Custodians following established policies and procedures.
2. Enable and Disable MFA for each Authorized User account.
3. Disable all Authorized User accounts found to be inactive for a period of 90 calendar days.
4. Delete all Authorized User accounts that have been disabled for a period greater than 1 year.
5. Respond to bureaus for specific help needed to audit City Technology Resource access.

Subsection 4 – Remote Network Access

Purpose

Remote network access is a generic term used to describe accessing the City's Technology Resources by Authorized Users who are not located within the City's facilities. Remote access may take the form of traveling Authorized Users, Authorized Users who regularly work from home, or Authorized Users who work both from the office and from home. In many cases, both the City and the Authorized User may benefit from the increased flexibility provided by remote access. As with any innovation, however, the benefits may be countered by risks if the purposes and methods of the remote access are not fully understood by all participants.

Internet-based, or "Cloud Services" Software as a Service (SaaS) services that contain City information are included within the scope of Bureau of Technology Services (BTS) Administrative Rules which apply to all City information repositories regardless of their storage locations or means of access. See **Subsection 19 – CLOUD SERVICES.**

The purpose of this policy is to define the approved methods for City Authorized Users to remotely connect to and access City Technology Resources and how these connections will be established, controlled and managed.

Administrative Rule

Remote access to City Technology Resources by Authorized Users is authorized when business activities require it, subject to approval by the Chief Technology Officer (CTO), the Senior Information Security Officer (SISO), or their delegate. The approved methods of remote access are through an authorized Virtual Private Network (VPN) connection from a

City-managed device, or resource-limited access to the City’s Microsoft Office 365 environment (Microsoft e-mail, Microsoft Teams, Microsoft OneDrive, or the Hitachi Anywhere portal.) with Multi-Factor Authentication (MFA).

The following additional policies apply to those Authorized Users approved for remote VPN access to City Technology Resources.

1. Remote network access must only occur via a BTS maintained and authorized virtual private network (VPN) system. A VPN is not required for the use of the City portal applications with secure access support, such as the City's web and Microsoft Office 365 portal. Full VPN tunnel access is only available to BTS maintained devices.
2. When actively connected to City Technology Resources, VPNs force all traffic to and from the remote device through the VPN tunnel. All other traffic is blocked unless City defined split-tunneling is established.
3. All VPN Authorized Users assume responsibility to assure that unauthorized users do not access City Technology Resources through their devices, software or configurations. This includes Authorized User's family members, friends, and associates.
4. Device security controls must be maintained to City standards in all unsecured remote locations.
    a. City-Managed Location: any City of Portland site with a City-managed network connection.
    b. Home Office: Teleworking from home, with VPN is allowed.
    c. Non-City Location: Not a City-Managed location or home office. Non-City locations are sites where BTS does not have administrative control over the network. VPN should always be active and more stringent security measures can be applied to devices connecting from these locations.
    d. Foreign countries: using City Technology assets in foreign countries is allowed by exception only. There are numerous security concerns to be aware of while traveling. Please submit a Helpdesk ticket with your itinerary for guidance prior to travel.
    e. Exceptions to the above require bureau director, CTO and SISO review and approval. Please work with your Business Relationship Manager to submit exceptions.

5. VPN connections offer a private connection into the City's network from the internet, therefore additional security measures are required to prevent unauthorized access, including but not limited to MFA. Personal devices are subject to increased security controls.

6. For non-City Authorized Users such as vendors and contractors, the responsible Business System Owners must identify remote technology resource access requirements with proper written justification of the business reasons for such access. Additionally, remote access for vendors or contractors must only be enabled during the time needed, disabled when not in use, and promptly deactivated after access is no longer

necessary. The SISO holds the final approval authority for all remote access to the City's network.

The following additional policies apply to Authorized Users approved for remote Office 365 access to City Technology Resources.

7. Bureau and BTS authorization are required for remote access to Office 365. Certain Authorized Users may have additional limitations related to remote access. See HRAR-4.04 - Telework and HRAR-4.08 - Information Technologies.

8. Office 365 access requires MFA when accessing City resources from unmanaged devices.

9. Office 365 access does not grant access to City resources and information stored within the City's physical environment (local file shares, databases, endpoint device disk drives, or local applications.

10. City information must not be saved or stored on devices that are not City-owned, managed, or have not been approved and governed by City contract. See HRAR-1.03 - Public Records Information, Access and Retention, and HRAR-11.04 - Protection of Restricted and Confidential Information.

11. City information and records must be managed in accordance with State and City Rules Related to Public Recordkeeping Requirements.

Exceptions to this policy, or any sections thereof, may be granted on a case-by-case basis by the CTO and the SISO. If an exception is granted for VPN technology on non-City devices, Authorized Users acknowledge that their devices are a de facto extension of the City's networks and as such, are subject to all policies that apply to City Authorized Users and City-owned and managed assets, including, but not limited to acceptable minimal security standards of operating systems and software.

Responsibilities

BTS is responsible for setting up remote VPN access in a manner that is consistent with Information Security standards and policies. Such standards and policies include current malware and endpoint protection software, approved operating systems, operating systems patches, active firewalls, as well as other security and remote administration tools.

Subsection 5 – Identity and Access Management

Purpose

Passwords are an important aspect of information technology security. Strong passwords are the front line of protection for Authorized User accounts. A poorly chosen password may easily result in the compromise of the City's entire Technology Resources. As such, all Authorized Users are responsible for taking the appropriate steps, as outlined below, to select and secure strong passwords.

The purpose of this policy is to establish a best practices-aligned standard for the creation of strong passwords, the protection of those passwords, the association of passwords with Authorized User accounts and the requirements for password changes and audits.

The scope of this policy includes all Authorized Users who have or are responsible for a City technology access account, regardless of device used or the location of the access account.

Administrative Rule

Password Standards

The City of Portland has updated City Password standards to align with the National Institute of Standards and Technology NIST SP 800-63-3 - Digital Authentication Guidelines, or as revised.

1. Each Authorized User is issued a single, unique City domain account and password. This account must be used for all City business. In general, sharing Authorized User accounts and passwords is prohibited. The Bureau of Technology Services (BTS) will work with bureaus who request an exception to this rule or to assist in implementing secure methods to address requirements met by sharing user accounts or passwords for limited access use cases.
2. Authorized Users are not permitted to reveal their passwords.
3. If an account or password is suspected to have been compromised, an Authorized User must report the incident to the BTS Helpdesk and change the password immediately.

See City of Portland Security Standards 4.0, *section 4.2 Password Requirements* for standards and usage guidance.

Password Protection

Reuse of City credentials and passwords is prohibited for non-City systems and Internet-based services (e.g., external email, etc.). City domain passwords must not be used for non-City purposes unless these accounts are managed through BTS’ enterprise account technologies (e.g. Active Directory (AD), Active Directory Federation Services (ADFS), or Single Sign-On (SSO) services).

1. The use of a password manager is recommended for secure storage of all City Authorized User passwords and account credentials.
2. KeePass is a BTS-approved standard. Contact BTS HelpDesk for guidance on authorized software installation and appropriate use.
3. Do not write passwords down or store them anywhere in your workspace. Do not store passwords in a file on any storage device without BTS approved encryption technologies.
4. Guidance list of "don’ts" for Password use and protection:

a. Don't reveal a password over the phone to anyone. BTS personnel will never ask for your passwords
b. Don't reveal a password in an email or text message
c. Don't reveal a password to your supervisor
d. Don't talk about a password in front of others
e. Don't hint at the format of a password (e.g., "my family name")
f. Don't reveal a password on questionnaires or forms
g. Don’t forget to use caution when completing on-line forms that request current or new passwords. Submission forms may be intercepted
h. Don't share a password with family members or friends
i. Don't reveal a password to co-workers while out sick, traveling or on vacation
j. Don’t use the "Remember Password" feature of technology applications and services (e.g., Microsoft Edge, etc.) as these leave your password vulnerable on the systems they are stored. This is a high-level security concern on shared systems such as kiosks or on an open wireless (Wi-Fi) network.

Password Discovery and Hardening

1. Password cracking or guessing may be performed by the Information Security Office on a periodic or random basis. If a password is guessed or cracked during one of these scans, the Authorized User will be required to change their password immediately.

Subsection 6 – Database Passwords

Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a software program or application that will access a database running on a City network or on City Technology Resources hosted outside of City networks.

Technology applications and services often require the use of database servers. To access these databases a software application or service must authenticate to the database by presenting authorized credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

This policy applies to all technology applications and services that access City Technology Resources production databases using stored credentials. An example of this scenario is a web server or batch processing system authenticating to a database server for the purpose of processing database queries on behalf of an Authorized User.

1. Database Password strength is governed by **Subsection 5 - IDENTITY AND ACCESS MANAGEMENT**and City of Portland Security Standards

4.0, *section 4.2 Password Requirements.*

2. BTS will work with bureaus who request an exception to this rule or to assist in implementing secure methods to address database password requirements.

Administrative Rule

General

1. To maintain the security of the City's internal or hosted databases, access by technology software applications and services must be granted only after authentication with valid credentials. The credentials used for this authentication must not reside in the main, executing body of the software application or service's source code in clear text. Stored authentication credentials must remain encrypted.

Specific Requirements for Database Passwords

Storage of Database Usernames and Passwords

1. Database usernames and passwords must be stored in a file separate from the executing body of the program's code. This file must not be world/everyone readable.
2. Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
3. Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP (Lightweight Directory Access Protocol) server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
4. Database credentials must not be stored in a location that can be accessed externally through a web browser.
5. Passwords or pass phrases used to access a database must adhere to **Subsection 5 - IDENTITY AND ACCESS MANAGEMENT.**

Retrieval of Database Usernames and Passwords

1. If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.
2. The scope into which database credentials may be stored must be physically separated from the other areas of code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
3. For languages that execute from source code, the credentials' source file must not reside in the same browse-able or executable file

directory tree in which the executing body of code resides.

Access to Database Usernames and Passwords

1. Each technology application and service function accessing a City managed or hosted solution (SaaS) database must have unique database credentials. Sharing of credentials between programs is not allowed.
2. Database passwords used by programs are system-level passwords as defined by **Subsection 5 - IDENTITY AND ACCESS MANAGEMENT.**
3. Database usernames and passwords used by technology software applications, services or programs, such as a web server connecting to a database, must not also be used for interactive sessions by end users or system operators.
4. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with **Subsection 5 - IDENTITY AND ACCESS MANAGEMENT**. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.
5. Access to database usernames and passwords MUST be from a limited number of authorized administrative endpoints and use MFA unless by exception.

Subsection 7 – Patching, Malware Prevention and Recovery

Purpose

Malicious software (malware) can be transferred over the Internet, by Mobile Devices, Removable Media, local area networks, email, and other means. Malware can quickly spread to destroy or corrupt data and valuable City information. Essential services for internal and external customers of City Technology Resources can be drastically affected by malware infections. To maintain high availability of City Technology Resources continuous efforts must be made to prevent malware infections.

This policy applies to all devices connected to City networks and hosted (SaaS) City Technology Resources to ensure effective malware prevention, detection and eradication. Devices may be City-managed or personal, smartphones, computers, portable storage devices, and network devices.

Any device or network connection that does not meet City security standards will be disconnected and prevented from accessing City Technology Resources.

Administrative Rule

All systems, devices, City-owned or personal, or Hosted Technology Recourses connected to City-owned and managed networks must have Bureau of Technology Services (BTS) approved malware protection software, operating systems, operating system patches, firmware, applications, and application patches installed, operational and up to date.

Responsibilities

Bureau of Technology Services Responsibilities

1. Maintain technology vulnerability and patch management program for continuous process improvement and to provide regular cybersecurity posture health and maturity status reports.
2. Maintain and review logs of repair and patching with approved and controlled tools.
3. Maintain the lifecycle of hardware, software, operating system, patches, firmware, and all technology equipment: procurement, installation, maintenance, patching, and monitoring of City assets.
4. Maintain vulnerability management tools and capabilities and scan City assets frequently for vulnerabilities and indicators of compromise.
5. Disclose detected Vulnerabilities to relevant parties and request patching in accordance with the severity of the vulnerability.
6. Maintain malware and threat prevention software in accordance with City standards and to institute measures to ensure that malware prevention methods remain current.
7. Patch management must be prioritized based on the severity of the vulnerability the patch addresses. Patching must meet applicable requirements within City of Portland Security Standards 4.0.
8. If patching cannot be completed in the timeframe listed in the above linked standards documentation, compensating controls must be put in place up to and including removal of unpatched devices from the network.
9. Maintain procedures for proactively preparing for and reactively responding to security incidents to minimize City impact and restore full operations as quickly and securely as possible.
10. Isolate or quarantine systems and/or network segments and Internet-based services to prevent and/or contain malware outbreaks, minimize impact and to effectively restore services in a timely manner.
11. Implement technologies and establish policies and procedures that limit the methods for connecting such devices and segmenting such devices (smartphones, computers, tablets, etc.) that do not meet City minimum security standards and specifications.

Bureau and Authorized User Responsibilities

1. Comply fully with all malware security actions, warning and notices as issued by BTS.
2. Work with BTS to patch vulnerabilities according to BTS Standards (insert link to standards doc), including scheduling downtime and coordinating outages with users and customers.

3. Immediately report all suspected malware incidents or missing/malfunctioning malware protection software to the BTS Helpdesk.
4. For Bureau-Supported hardware, software, or operating systems, patching must be completed on the same scheduled that applies to BTS according to the City of Portland Security Standards 4.0.
5. Bureaus are responsible for funding the replacement of bureau-owned devices when they no longer support BTS policies or standards required to maintain security and patching on such equipment. BTS may take preventive action to protect the City network from devices which are bureau-supported and non-compliant. This may include firewalls, segmentation, and other security implementations.
6. As noted in HRAR-4.08 - Information Technologies do not download and/or install any software (including free or trial software) on City devices without prior BTS approval.
7. Do not connect any non-BTS supported device to the City network without prior BTS validation and authorization.
8. Do not circumvent, disable, or remove any BTS malware protection software, systems or patches.

Use of personal and non-City devices to access City Technology Resources

1. Personal devices may connect to cloud hosted City Technology Resources, such as Microsoft Office 365, when following all applicable City of Portland BTS, Bureau of Human Resources and City of Portland Auditor's Office Administrative Rules.
2. Personal devices are not allowed to connect directly to the City network. Devices not secured and maintained by the City to BTS security standards present unpredictable risks.
3. Remote users may use SSL VPN from personal devices that meet City security controls.

Supporting Practices

With assistance from the Bureau of Technology Services, bureau and office managers must ensure that Authorized Users are provided with information on safe practices for malware protection and that these safe practices are always observed.

As per HRAR-4.08 - Information Technologies, City Authorized Users are reminded of the expectation to observe safe practices regarding the use of devices to minimize malware risks.

Subsection 8 – Incident Reporting and Response

Purpose

Security compromises can potentially occur at every level of computing from an individual's desktop computer or mobile device to the largest and best-protected technology systems within the City. Incidents can be accidental incursions or deliberate attempts to compromise City Technology Resources and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact on the security of individuals, business services, systems and the City as a whole.

For the purposes of this policy an "Information Security Incident" is any accidental or malicious act with the potential to a) result in misappropriation or misuse of Confidential or personal information (compliance information, such as PCI, CJIS, FTI; attorney client privileged information, social security numbers, health records, financial transactions, etc.) b) imperil accessibility to or the functionality of City Technology Resources, c) allow unauthorized access to City resources or information, or d) allow City Technology Resources to be used to launch attacks against the resources and information of other individuals or organizations.

In the case an Information Security Incident is determined to be of potentially serious consequence, the responsibility for acting to resolve the incident and to respond to any negative impact rests with the BTS Information Security Office in cooperation with the Chief Technology Officer (CTO) rather than other specific individuals, bureaus, departments, or groups. The City has established procedures and identified the Senior Information Security Officer (SISO) as its authority in developing response plans to serious Information Security Incidents. As described below, reports of Information Security Incidents will immediately be forwarded to the SISO. The SISO follows protocols in determining what actions must be taken and depending upon the nature of the security incident will determine whether incidents should be handled within the purview of the affected bureau, Bureau of Human Resources (BHR), or by additional security and operations specialists within BTS, the Information Security Office, or through partnership with external information security incident response resources. In certain cases, the SISO may escalate the incident to the City Attorney’s Office, law enforcement, BHR, Risk Management or other City officers.

This policy outlines the procedures Authorized Users must follow to report potentially harmful Information Security Incidents. Authorized Users whose responsibilities include managing computing and communications systems have even greater responsibilities. This policy outlines their responsibilities in securing systems, monitoring and reporting Information Security Incidents, and assisting Authorized Users, Business System Owners, Data Custodians, System Operators and Administrators, and BTS staff to resolve security incidents.

Administrative Rule

All Authorized Users must take appropriate actions to immediately report and minimize the impact of Information Security Incidents.

Reporting unlawful or improper actions of Authorized Users is expected and covered in the following Bureau of Human Resources Administrative Rules:

HRAR-4.08 - Information Technologies

HRAR-11.01 - Statement of Ethical Conduct

HRAR-11.02 - Prohibited Conduct | Portland.gov

HRAR-11.03 - Duty to Report Unlawful or Improper Actions

Human Resources Administrative Rules

Responsibilities

Authorized Users

1. Report Information Security Incidents immediately to the BTS Helpdesk by phone 503.823.5199. BTS support staff will help you assess the problem and determine how to proceed.
2. Do not delete anything unless told to do so.
3. Following the report, individuals must comply with directions provided by BTS support staff and/or the SISO to repair the system, restore service, and preserve evidence of the incident.
4. Individuals must not take any retaliatory action against a system or person believed to have been involved in an Information Security Incident.

BTS Support Professionals

BTS Support Professionals have additional responsibilities for Information Security Incident handling and reporting for the systems and services they manage. In the case of an Information Security Incident, BTS support staff must:

1. Respond quickly to reports from individuals.
2. Take immediate action to stop or contain the incident from continuing or recurring.
3. Following BTS Incident Response protocols and established procedures determine whether the incident should be handled locally or reported to the SISO.
4. Analyze impact of incidents according to the criticality (threshold) of the event by performing forensic analysis.
5. Use all available logs, data and other tools to assess the criticality of the incident.
6. Respond to incidents within the context of Continuity of Operations, Contingency, and Disaster Recovery Plans.

7. Once the incident is understood, it will be mitigated, and response processes will be updated with lessons learned.
8. If the incident involves the loss of City Confidential and Restricted Information, including personal information, critical data, or has potentially serious impacts for the City, the BTS Support Professional must:
    a. Contact the Information Security Office immediately. The SISO or a delegate will investigate the incident in consultation with the CTO and relevant technology support specialists and develop an Incident Response plan.
    b. File a report, using BTS' service ticketing system, including a description of the incident and documenting any actions taken. The Information Security Office may request BTS Support Professionals to complete an *Information Security Incident report form*.
    c. Do not discuss the incident with others until a response plan has been formulated. The SISO and the appropriate Principal Information Officer will determine information disclosures and notices.
    d. Follow the Incident Response plan to preserve evidence of the incident, repair the system(s) and restore services.
    e. Manage public relations and ensure reputation is repaired after an incident.

Subsection 9 – Mobile Devices and Removable Media

Purpose

The purpose of the City's Mobile Devices and Removable Media security Administrative Rule is to establish rules for the use of Mobile Devices and Removable Media and their connection to the City's networks and authorized Internet-based Service Provider hosted services. These rules are necessary to preserve the integrity, availability and confidentiality of City information and technology assets.

Administrative Rule

1. Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and are portable (i.e., non-stationary). These devices come in various forms such as: smartphones, smart watches, tablets, laptops, and wearable devices.
2. Mobile devices must follow all relevant City Administrative Rules and Information Security Administrative Rules.
3. Only Bureau of Technology Services (BTS) approved Mobile devices and Removable Media may be used to access City information systems and resources. The BTS Infrastructure Board, administered by BTS' Enterprise Architecture, approves Technology Standards.

4. Employees may not download City information onto personal devices. The download of City data to personal devices exposes employees to the possibility of subpoena or Records Requests.
5. City Confidential Information stored on Mobile Devices or Removable Media must use BTS approved encryption techniques for temporary data storage. Please see **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING**for more information on the definition of Confidential and Restricted information.
6. City Confidential and Restricted Information must not be transmitted via wireless technology to/or from a Mobile Device unless BTS approved encrypted wireless transmission protocols are implemented. See also **Subsection 10 - WIRELESS NETWORKS.**
7. Sharing devices will be evaluated by BTS, to ensure tracking of device ownership, licensing, and accountability, authorization, and authentication. Single-user devices (smartphones and similar devices incapable of authenticating multiple users) cannot be tied to multiple user accounts and identities.
8. Mobile devices and Removable Media must have BTS approved storage encryption, anti-malware capability, and device firewall operational and always activated.
9. Mobile devices that cannot support the requirements of**Subsection 5 - IDENTITY AND ACCESS MANAGEMENT**are required at a minimum to implement a six-digit PIN with a fifteen-minute inactivity lockout.
10. Use of synchronization services, such as backups, for mobile devices (e.g., local device synchronization, remote synchronization services, and websites) must be controlled through a Mobile Device Management (MDM) or other centralized management solution.
11. Mobile devices may not access City networks unless their integrity is verified (including whether the device has been rooted/jailbroken, software patches, OS patches, etc.).
12. All remote and mobile device access to City networks and authorized Internet-based Service Provider hosted services must comply with the requirements of **Subsection 4 - REMOTE NETWORK ACCESS.**
13. Non-City owned mobile devices and remote access services that require City network connectivity must conform to City information security policies and standards. Non-City owned or managed mobile devices may have limited access rights to City technology resources and information.
14. All City Authorized Users must secure Mobile Devices and Removable Media in their care and possession and immediately report any loss or theft of such devices to their bureau management and BTS HelpDesk. Additionally, if such devices support connectivity to City networks, the BTS Helpdesk 503-823-5199 must be contacted to take immediate steps to protect against unauthorized access to the City's Technology Resources.
15. Exceptions to this Administrative Rule must be approved in writing by the Chief Technology Officer (CTO) or the Senior Information Security Officer (SISO).

Subsection 10 – Wireless Networks

Purpose

This policy prohibits access to City Trusted Networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy and City Information Security Standards and Administrative Rules or those Authorized Users which have been granted an exclusive waiver by the Chief Technology Officer (CTO) or the Senior Information Security Officer (SISO) are approved for connectivity to the City's Trusted Networks.

This policy covers all wireless information communication devices, whether City managed or personally owned (e.g., computers, laptops, notebooks, smartphones, tablet computers, etc.) which connect to any of the City's networks, or authorized Internet-based Service Provider hosted services, technology resources, or City managed or connected systems.

Administrative Rule

1. Wireless networks must follow all requirements of information security policies, standards, and City Administrative Rules including, but not limited to, a risk assessment prior to implementation.
2. Register Network Infrastructure Wireless Devices: All network infrastructure wireless devices (Access Points, Base Stations and Network Interface Cards) connected to City networks must be approved, registered, installed and maintained by the Bureau of Technology Services (BTS).
3. Encryption and Authentication: To connect to City networks, all networking devices with wireless capabilities must utilize a City approved configuration which prohibits all unauthenticated and unencrypted traffic.
4. Wireless networks must use the strongest encryption available.
5. All Wireless Network device implementations must support a hardware address (MAC address) or BTS approved unique device identifier (Certificate or other) that can be registered and tracked.
6. All wireless implementations must support and employ strong user authentication which checks against BTS approved and managed Identity and Access Management stores using approved Authentication Protocols and procedures.
7. Setting the Service Set Identifier (SSID): All wireless access points must have their SSID configured so that it does not contain the default authentication credentials supplied by the manufacturer or disclose the manufacturer or model information.
8. Wireless security measures must be applied to all wireless networks, such as, but not limited to Intrusion Detection Systems (IDS).
9. Public wireless networks must be, at a minimum, physically separated from the internal network or configured to tunnel to a secure endpoint outside the internal network. The design must be included in the documented security plan.

10. The wireless network administration console must not be directly accessible from the wireless network.
11. Penetration Tests and Audits: Wireless Access Points and Base Stations are subject to periodic penetration tests and audits. Unauthorized Wireless Access Points are subject to immediate network disconnection and equipment confiscation.
12. Default wireless manufacturer or vendor settings must be changed, including but not limited to default wireless encryption keys, passwords and SNMP community strings.

Subsection 11 – Analog Modems

Purpose

This policy explains the City's analog modem acceptable use and approval rules and procedures. This policy covers the use of modems that are connected to City Trusted Networks and City Technology Resources.

This rule applies only those modems that are connected to a device or networks within City owned or occupied facilities.

There are two important scenarios that involve modem misuse which BTS attempts to guard against through this policy. The first is an outside attacker who calls a set of phone numbers in the hope of connecting to a device which has a modem attached to it. If the modem answers from inside City premises, there is the possibility of breaching the City's internal networks through that device. At the very least, information that is held on that device can be compromised. This potentially results in the loss of City Confidential and Restricted Information.

The second scenario is the threat of anyone with physical access to a City facility being able to use a modem equipped device. In this case, the intruder could connect to City Trusted Networks of the City through the device's Ethernet connection and call outbound to an unmonitored site using the modem, with the ability to exfiltrate City information to an unknown location. This could also potentially result in the substantial loss of Confidential and Restricted Information.

Administrative Rule

All requests for analog communication access – into or exiting from City Trusted Networks – require preapproval from the Chief Technology Officer (CTO) or Chief Information Security Officer (SISO).

Procedure

Requesting a Modem Connection

The requester must submit a service request to the BTS HelpDesk. Guidance and resources are available at BTS - Secure Virtual Private Network (VPN) Secure Remote Access.

The CTO or SISO will review and rule on all analog modem requests.

Once approved by a Bureau Director, the individual requesting a modem connection must provide the following information:

1. A clearly detailed business case of why other secure connections available within the City cannot be used.
2. The business purpose for which the modem is to be used.
3. The software and hardware to be connected to the analog phone line and used across the line.
4. To what external connections the requester is seeking access.

The business case must answer, at a minimum, the following questions:

1. What business services will be conducted over the modem?
2. Whether any City Confidential or Restricted Information is transmitted?
3. Why a City equipped desktop computer with Internet access capability is unable to accomplish the same tasks as the proposed modem?

In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:

1. Will the devices that are using the modem be physically disconnected or network segmented from City's internal network?
2. How will the modem be secured? Where will the modem be placed? An office, cubicle, or lab?
3. Is dial-in from outside of the City required? If so, what authentication controls or audit logs are in place to prevent unauthorized remote access?
4. How many modems are being requested, and how many Authorized Users will use them?
5. How often will the modem be used? Once a week, 2 hours per day, etc.?
6. What is the earliest date the modem can be terminated from service as the modem must be removed as soon as it is no longer in use?
7. What means will be used to secure the modem from unauthorized use?
8. What types of protocols will be run over the modem and analog line?

Device Configuration Requirements:

1. BTS will install approved endpoint detection and response (EDR) software on the device(s) using the modem.

Subsection 12 – Physical Security and Assets

Purpose

This policy describes the methods and responsibilities for protecting Citywide physical computer, network, communications and City Technology Resources. The City requires that appropriate environmental controls, physical protection and access controls be in place to protect computing and information resources. Proper and adequate physical security and protection is the responsibility of all City Authorized Users.

Physical Security

Physical security measures are an important part of any effort to protect City Technology Resources and City technology services, which include hardware, software, physical storage media and printed materials, and access security controls. Physical security control measures will be applied in accordance with physical and environmental considerations, compliance regulations, information privacy and confidentiality, and service criticality.

Public Areas

1. City of Portland physical locations where the public may enter without restriction.
2. Areas with kiosk computers or bill pay stations.
3. Customer service counters.
4. Public meeting rooms.
5. Any other location the public is welcome.

Restricted Areas

1. Small sets of individual Bureau servers located in office and remote location environments.
2. Computer labs which host computing and network equipment used for testing and development purposes.
3. Telecommunications closets which contain network and communications equipment and wiring.
4. Media storage areas and vaults which are used to store electronic media such as backup disk drives, surplus equipment, as well as classified and archival documents.
5. Modest-sized server rooms which host a limited number of computing devices and networking equipment.
6. Enterprise data center facilities that host a wide variety and large quantity of critical computing equipment such as technology appliances, servers, data libraries, information storage arrays and network equipment.
7. Internet-based Service Provider services that provide software as a service (SaaS) and information technology services that extend the City’s networking environment.
8. Any area where Criminal Justice Information (CJI) is processed.

Regardless of the specific environment, the City requires physical security requirements to be supported by all Business System Owners, Data Custodians, System Operators, and Authorized Users.

Assets

1. Physical technology assets include but are not limited to servers, routers, switches, load-balancers, firewalls, workstations, laptops, tablets, smart phones and any physical technology device that holds or transmits City data.
2. Software, including all applications used on City systems, Software as a Service, Platform as a Service, Infrastructure as a Service, or other applications hosted in a 3rd party cloud.
3. Cloud-based solutions hosted in City-managed or owned public clouds.
4. Containerized Servers.

Supply Chain

1. Supply Chain is how products or assets are acquired, including multiple tiers of procurement, ordering, contracting, logistics and manufacturing.
2. The Supply Chain needs to be understood to accurately assess risks to it, and plan for impacting events.

Administrative Rule

At a minimum, the following physical security measures and objectives must be implemented where applicable to protect City Technology Resources, and City Confidential and Restricted Information:

1. All technology assets, both physical and virtual (hardware, software, and any other construct that interacts with the City's network), must have an asset tag or a unique identifier which will be tracked in a centralized data repository.
2. Access keys and key codes to restricted areas must be limited to only those individuals needing entry to fulfill their job responsibilities. Records of individuals' assigned access must be maintained. Access logs must be maintained for at least one year, at a minimum, or if applicable regulations require. Access approval shall be 'minimum necessary' and 'need to know' in keeping with regulatory and applicable City Administrative Rules.
3. Technology appliances, servers, network equipment, computer media containing City Confidential and Restricted Information and other essential computer and network devices must be stored in a secure location, such as a locked room, that protects them from unauthorized physical access, use, misuse, destruction or theft.
4. Smoke/fire alarm and suppression systems are required for all data centers, server rooms and telecommunication closets to mitigate personnel harm and/or damage to City Technology Resources in the event of a fire.

5. Temperature and ventilation control measures are required for all data centers and server rooms to protect City Technology Resources from preventable service disruptions or physical harm from negative environmental conditions.
6. All mission critical data centers must employ emergency power control systems (backup generators and uninterruptible power supplies) to avoid disruptions and/or equipment/data harm due to power related failures.
7. Inventory control measures such as inventory reports, asset tags or other identification markings for tracking are required per City accounting policy.
8. All access to restricted areas, such as data centers, server rooms, and telecommunications closets, by unauthorized individuals must always be conducted with an authorized City employee escort.
9. All specific tools, systems, or procedures implemented to meet physical security requirements must be selected based on importance to safety, information and physical security and compliance with City Administrative Rules, policies and standards.
10. Each technology purchase should have the Supply Chain identified and tracked. (Supply Chain - NIST.gov).
11. Component authenticity should be verified.
12. Purchasing technology from federally or locally prohibited sources is not permitted.
13. Supply Chain for critical assets must be tracked, and a Supply Chain Risk Management Plan should be created to prepare for critical events.
14. If an asset is lost or stolen, report the loss to BTS and file a police report if stolen.
15. Data, as an asset, should be destroyed according to the level of classification assigned. See **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING**

All Authorized Users must be responsible to secure City Technology Resources in their care and possession and immediately report any loss or theft of such assets to their management and the BTS HelpDesk. Additionally, all Authorized Users must be aware of Unauthorized Users (e.g. maintenance, public and others visiting, delivery personnel, vendors, etc.) and be prepared to challenge individuals entering data centers, computer rooms and other restricted areas. Attempts by Unauthorized Users to access City Technology Resources or facilities must be reported to the OMF Facilities Security office.

Subsection 13 – Intrusion Prevention and Detection

Purpose

Intrusion prevention and detection plays an important role in implementing and enforcing the City's Information Security policy. As information technology services and systems grow in complexity, effective security protection systems must mature. With the proliferation of cybersecurity vulnerabilities introduced by use of internetworking technologies a level of assurance is needed that City Technology Resources are secure. Intrusion prevention and detection systems provide an essential part of that assurance.

The City Intrusion Prevention and Detection policy applies to all Authorized Users and all access to City Technology Resources. Additional responsibilities are assigned to technology support and administrative roles that are responsible for the installation of new information technology systems and services, the operations of existing information technology systems and services, and Authorized Users charged with information security.

Administrative Rule

1. Analyze threat alerts, threat detections and threat intelligence on a regular basis.
2. Operating system, user accounting, and application software audit logging processes must be enabled on all endpoint (host), Internet-based Service Provider (cloud) and server systems.
3. Active scanning, packet captures, and TLS inspection is used to investigate and proactively detect and stop malicious activity.
4. Alarm and alert functions of all firewalls and other network access control systems must be enabled.
5. Audit logging of all firewalls and other network access control systems must be enabled.
6. Audit logs from the access control systems must be monitored and reviewed by the service or system operators.
7. Service and system integrity checks of the firewalls and other network access control systems must be performed on a routine basis, as approved by the Information Security Office.
8. File, file system, firmware and OS integrity must be monitored and verified.
9. Software control. Create an allow or deny list of approved and prohibited software, scripts and code, including mobile device code and software.
10. Audit logs for services, servers and hosts on the internal, protected, network must be reviewed by the responsible BTS Support Professionals, Business Systems Owners, or System Operators and System Administrators.
11. Audit logs for Internet-based Services Provider services must be reviewed by accountable City Authorized Users as defined within the terms of the service contract, applicable regulations, City and BTS policies and Administrative Rules.
12. System Operators and System Administrators will furnish audit logs to the Information Security Office upon request.
13. Audit log review, in conjunction with event correlation software, may be delegated to authorized service and system technical custodians.

14. Endpoint-based (host) threat detection and response (EDR) and network-based intrusion prevention and detection tools must be audited on a routine basis as required by applicable regulations, City and BTS policies and Administrative Rules.
15. All critical and high threat alerts and reports of anomalous activity must be reported to and reviewed by BTS Support Professionals for symptoms that might indicate unauthorized access or cyber threat activity. The Information Security team will assess whether an Incident Response plan activation is warranted.
16. All suspected or confirmed instances of unauthorized access, misuse or abuse of City Technology Resources must be immediately reported by Authorized Users and BTS staff according to **Subsection 8 - INCIDENT REPORTING AND RESPONSE.**

Subsection 14 – Security Assessments, Audits and Penetration Tests

Purpose

This policy outlines the authority for Authorized Users of the City's Information Security Office to conduct security audits, monitoring, and investigations of technology systems within and connected to City Trusted Networks. The Information Security Office is also authorized to request third party Service Providers provide annual third-party security audit reports and all findings for anomalous activities and suspected security compromises.

Audits may be conducted to:

1. Ensure integrity, confidentiality and availability of information and City Technology Resources.
2. Investigate possible Security Incidents and ensure compliance with mandatory regulations and City information security policies and Administrative Rules.
3. Monitor user or system activity where appropriate, and to detect and prevent unauthorized access to City Technology Resources.
4. Develop Risk Assessments related to compliance, including but not limited to Criminal Justice Information (CJI) or Federal Tax Information (FTI).
5. Develop Disaster Recovery, Continuity of Operations and Contingency Plans.
6. Conduct Supply Chain risk assessments.

This policy applies to all technology devices owned or operated by the City and any non-City owned, personal technology devices that are present on City owned premises or are connected to City Trusted Networks and may not be owned or operated by the City.

Administrative Rule

When City Information Security Office Authorized Users conduct information security audits, investigations, penetration tests and activate Incident Response plans, City personnel must, upon request, provide appropriate and timely information and access to applications, systems and facilities. This policy does not supersede the requirement that the City auditor or other appropriate Bureau Directors approve access to City Technology Resources, such as when restricted by law or State and Federal requirements.

Audit and investigation access by the Information Security Office may include:

1. Authorized User level and/or system level access to any City or personal technology device accessing City Technology Resources.
2. Access to information (electronic, hardcopy, etc.) that may be produced with, transmitted through or stored on City Technology Resources.
3. Access to City owned and managed work areas (data centers, computer rooms, telephone closets, labs, offices, cubicles, storage areas, etc.).
4. Access to interactively monitor and log traffic on City Trusted Networks.
5. Access to information to inform Risk Assessments, Risk Management and Risk Tolerance.

The City is subject to several State and Federal cybersecurity compliance requirements that mandate routine audits by the City. The City's Information Security Office performs internal compliance audits and investigations in support of the City's regulatory compliance and Administrative Rules.

Certain Information Security threat identification capabilities, systems and services automatically perform security analyses that are designed to alert BTS and Authorized Users to Security Incidents, cybersecurity threats, technology system failures, and out-of-policy activities.

Subsection 15 – Encryption

Purpose

Encryption standards and technologies are used to prevent Unauthorized Users from accessing or altering Confidential or Restricted Information stored on City Trusted Networks and City Technology Resources, Hosted Technology Resources, or transmitted across City and public networks.

The purpose of this policy is to provide guidance for where encryption technologies must be implemented and limit the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that State and Federal regulations are observed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Administrative Rule

Applicability

Approved encryption standards and techniques for the storage and transmission of City Confidential and Restricted Information must be implemented based on a) information classification, as defined in **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING** and, b) information security risk management decisions established by the Chief Technology Officer (CTO), Senior Information Security Officer (SISO) and Business System Owner, unless expressly required and defined by regulation, statute or contractual obligation.

The following classifications of Confidential and Restricted Information are expressly subject to the City's Encryption policy:

1. Criminal justice information (CJI) when transmitted across public networks or any private network that is shared with non-criminal justice Authorized Users.
2. Authorized User or application-level credentials (account names and passwords).
3. Payment Cardholder Data (PCI) including primary account number, cardholder name, expiration date, and service or security code or Personal Identification Number (PIN)
4. Personally identifiable information (PII) as defined by the Oregon Consumer Information Protection Act.
5. Electronic protected health information (PHI) such as health benefit information covered under HIPAA privacy regulations.
6. Any 802.11 wireless or Remote Network Access communications when used to connect to the City's Trusted Networks or City Technology Resources.
7. Confidential and Restricted Information stored on Mobile Devices, such as laptops, smartphones, and Removable Media, such as USB thumb drives.

Note: This is not a complete list and is provided to give general guidance for commonly used Confidential and Restricted Information which are subject to higher levels of information security protection. Please contact the BTS Information Security Office for appropriate classification of data and to help determine if encryption is required. See also **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING.**

Additional Compliance Considerations

1. Where networks and systems are under legal regulations such as Criminal Justice Information Systems (CJIS) standards, there may be additional encryption requirements above and beyond the City's encryption policy.

2. Criminal Justice Information is restricted to authorized United States agency use within U.S. borders.

Subsection 16 – Firewall and Security Systems

Purpose

This policy describes the methods and responsibilities for securing City Trusted Networks, City Technology Resources, and City Confidential and Restricted Information. Specifically, this policy outlines the standards and authority for managing the City's Trusted Networks and cybersecurity threat detection, prevention, and defense systems.

Administrative Rule

Information Security is responsible for developing all policies, standards and configuration change controls for the implementation, and use of firewalls and security systems within the City. These policies and standards include but are not limited to:

1. At minimum, a stateful packet inspection firewall is required at each Internet and external connection, and additional security features will be enabled as needed.
2. Firewalls are required between security boundaries or Security Zones, including boundaries between the City and external entities, and between internal City systems with different security levels or purposes.
3. Firewalls will be used to enforce security between subnets, and to enable network segmentation.
4. Management, administrative, and other Confidential networks should be protected by firewalls.
5. A stateful packet inspection firewall is required between any Demilitarized Zone (DMZ) and/or Security Zone and the City's Trusted Networks and City Technology Resources.
6. A stateful packet inspection firewall is required on either side of resources shared between the City and external partners to form a DMZ between the two entities networks. These firewalls must be physically separate devices or clusters when protecting networks managed by two different groups, or creating DMZs for high security systems, including external networks, Industrial Control Systems, or other critical infrastructure.
7. A stateful packet inspection firewall must reside between the Internet and any City system, resource or network-connected device. Inbound Internet traffic must be limited to DMZs that include security systems and capabilities which provide authorized publicly accessible services.
8. Determination of Standard Changes and Risk Assessments for firewall rule additions, change, and exceptions.
    a. Additional Firewall Standards are defined within City of Portland Security Standards 4.0.

9. Firewalls must be configured to specifically deny traffic that has not been approved and documented.
10. Firewall rules must be reviewed by BTS firewall administrators at least once every six months to ensure the rules' accuracy and continued necessity.

Intrusion Detection and Prevention

Intrusion Detection and Prevention Systems (IPS/IDS) must be implemented at network perimeters and critical network access points, and where deemed necessary for compliance, and must alert appropriate BTS Support Professionals and BTS Support Staff to suspicious network activities, incidents or malicious behavior.

Firewall Rule Change and Exception Requests

Written justification is required to provide a connection through a firewall. Business Systems Owners must submit written documentation for all access changes required to conduct their business. Submitted documentation must include the business reasons for these changes and the end date for this business need.

1. Information Security approves or denies all requests to modify the City's cybersecurity posture and for allowing additional protocols, services and access to City Technology Resources.
2. BTS firewall administrators evaluate all requests for firewall rule changes and maintain all required documentation on the business need for the firewall rules.
3. Requests for additional firewall rule and protocol changes from external and/or untrusted networks are not permitted without written justification from Business Systems Owners and approval from the Information Security Office.

Subsection 17 – Payment Card Industry Data Security Standards

Purpose

The City collects payments using payment cards (credit and debit cards) for a variety of purposes. The payment cardholder association (Visa, Mastercard, American Express) requires that the City abide by specific information security standards, known as Payment Card Industry Data Security Standards (PCI DSS) for permission to process electronic payments using various payment cards.

This administrative rule outlines specific PCI DSS requirements related to payment card process environments managed and secured by the City and Authorized Third-Party PCI Payment Processors City payment card environments include any City systems, networks, applications and services that transmit, store, or process City payment cardholder data.

Administrative Rule

1. The City and its PCI Payment Processors must meet all applicable requirements of the current PCI DSS standard, as set forth by the PCI Security Standards Council (www.pcisecuritystandards.org). The 'in-scope' requirements are determined by one or more Self-Assessment Questionnaire (SAQ) types depending on the modes and means of services within each payment card environment. Understanding the SAQs for PCI DSS version 3
2. Bureaus that use City-approved PCI Payment Processors for electronic payment processing services must use only services and software that are Payment Application Data Security Standard (PA DSS) compliant.
3. PCI DSS includes a broad expanse of general and overarching information security standards, technology controls, and behavioral expectations that are addressed in other City Administrative Rules of Bureau of Human Resources, Office of Management and Finance, and additional Administrative Rules.

Citywide Technology Standards for PCI DSS Compliance

The following PCI DSS Citywide technology and process standards are required for the City to achieve and maintain compliance with PCI DSS. These standards include but are not limited to:

Payment Card Services Roles and Responsibilities

1. The City is required by the PCI Council to contract with an external PCI-certified auditor to conduct annual risk and compliance assessments of the City's payment card environments.

2. The City is also required to secure a contract for an annual independent PCI DSS compliance audit and quarterly network scans of all bureaus, technologies, and platforms that process electronic payments.

3. The City is also required to annually confirm and collect Attestations of Compliance (AOCs) from all City Authorized Third-Party PCI Payment Processors.

4. Active City participants in PCI risk assessments include each PCI service Business System—or service—Owner (Bureau or Office), Data Custodian (Merchant ID Manager (MID Manager), OMF Treasury Division, BTS Support Professionals - BTS Support Staff, and the Information Security Office.

5. The City Treasury Division is the PCI program service owner, and the Information Security Office is the technical controls compliance process owner.

6. Each bureau that provides payment card services or supports a payment card environment must develop and maintain service-specific policies, processes, procedures, training, and security controls to maintain PCI compliance for services within their scope of responsibilities.

7. The Information Security Office must conduct an annual review of its security policy as it relates to City payment card environments and update the policy whenever changes in the cardholder environments or PCI rules necessitate a change.

Authorized Third-Party PCI Payment Processors

1. Business Systems Owners and the OMF Treasury Division must maintain a current list of Authorized Third-Party PCI Payment Processors.

2. Business Systems Owners and the OMF Treasury Division must maintain a written agreement that includes an acknowledgement that Authorized Third-Party PCI Payment Processors are responsible for the security of cardholder data they possess or otherwise store, process or transmit on behalf of the City.

3. Business System Owners and the OMF Treasury Division must establish a program to annually confirm Authorized Third-Party PCI Payment Processors' PCI DSS compliance status.

4. Business System Owners and the OMF Treasury Division must maintain information about which PCI DSS requirements are managed by each Authorized Third-Party PCI Payment Processors, and which are managed by the City of Portland.

Authentication

1. Shared passwords are prohibited to access any payment card environment, system, application, service or Trusted Networks.

Activity and Log Monitoring and Incident Response

1. All Authorized Users must report Information Security Incidents immediately to the BTS Helpdesk. BTS support staff will help you assess the problem and determine how to proceed. See: **Subsection 8 - INCIDENT REPORTING AND RESPONSE**for processes and procedures.

2. Information Security personnel and BTS Support Professionals - BTS Support Staff provide 24 by 7 Incident Response and monitoring coverage for any evidence of unauthorized activity or Information Security Incidents. This monitoring coverage includes resilient communications tools, such as email or text alerts, that provide timely information on the status of secure transmission, storage, or processing of payment card data.

3. All transaction and activity logs from relevant systems within the City payment card environments must be reviewed daily.

4. Logs from payment card environments systems must be retained for one year from their creation date.

5. Logs include, but are not limited to, user identification, type of event, date and time, access success or failure indication, origination of an event, identity or system component of affected data, or resources.

6. Payment card environment systems or services that support event correlation must maintain audit trails to associate all access to system components or services with Authorized User accounts.

Physical Access

1. Physical access to equipment processing cardholder data must be restricted. Access must be authorized and based on individual job function, and be revoked immediately upon termination, including but not limited to the recovery or disabling of all keys, access cards, etc.

2. Storage of all payment card data in electronic systems or physical media will be kept only to complete the payment transaction and will not be stored longer than business needs require. At no time after card authorization, under any circumstance, will the Citystore any information from the card magnetic track, the Card Validation Value/ Card Validation Code CVV/CVC, CVV2/CVC2, or the Personal Identification Number (PIN) block data.

3. Paper copies of payment cardholder data must be cross-cut, shredded, incinerated, or pulped once they are no longer needed.

4. Physical storage of electronic and physical media containing payment cardholder data must be secured in locked containers within physically secured, non-public-access, workspaces.

5. End-of-life electronic media used to store payment cardholder data must be purged, degaussed or destroyed so that cardholder data cannot be reconstructed.

6. All electronic systems and physical media with cardholder data will be audited on a quarterly basis to ensure that stored classified data does not exceed business retention requirements and that the retention schedule is adhered to.

Payment Card Services Device Management

1. Only devices authorized by the Information Security Office must connect to City managed payment card systems, applications, services or environments.

2. Bureaus that use payment card devices to process payment card transactions must use only devices that meet PCI PIN Transaction Security (PTS) validation and utilize point-to-point encryption technology.

3. All payment card environment modems must automatically disconnect after 15 minutes of inactivity.

4. All payment card systems, devices, applications or services that transmit, store, or process cardholder data must be properly inventoried, secured, and where appropriate, labeled.

5. The OMF Treasury Division maintains the Citywide database of authorized payment card processing environments, devices, current Business System or Service Owner, MID Managers, Merchant IDs, and Authorized Third-Party PCI Payment Processors.

6. MID Managers are responsible for providing the OMF Treasury Division with all payment card services information and all changes within their payment card environment, including, but not limited to: contact information, and purpose of the system or device.

7. Payment cardholder data is prohibited from transmission via end-user messaging technologies including, but not limited to, email or text messaging.

8. A current list of all systems or devices that transmit, store, or process cardholder data must be maintained by each Bureau, Office or MID Manager and the OMF Treasury Division.

9. The physical locations for all payment card systems or devices must be reviewed at least annually and approved by the Information Security Office.

10. Time synchronization technology must be used to maintain a correct and consistent time within critical systems. Changes to time configuration must be protected and initiate an alert.

11. Vulnerability scanning will be conducted on a regular basis and after any significant change for PCI scope devices including but not limited to desktops, servers and network devices. Any PCI scope devices that are discovered to have vulnerabilities must be remediated according to the schedule enumerated in the BTS Patch Management Standards. See: City of Portland Information Security Standards

12. Public-facing web applications must be assessed and protected against new threats through vulnerability security assessments at least annually, or an automated technical solution that detects and prevents web-based attacks.

Stored Cardholder Data

Retention or storage of authentication data after authorization--even if encrypted—is prohibited. When authentication data is received, render all data irretrievable upon completion of the authorization process.

Retention or storage of any cardholder data from a chip or magnetic track--the magnetic stripe located on the back of a card–is prohibited.

Retention or storage of the personal identification number (PIN) or the encrypted PIN block is prohibited.

Retention of any permitted cardholder data must be securely stored by implementing data retention and disposal policies, procedures and processes that include at least the following:

A. Limiting data storage content and retention time to that which is required for legal, regulatory, and business requirements,

B. Establishing and maintaining processes for secure deletion of data when no longer needed,

C. No permitted cardholder data may be stored or copied onto personal computers, or any other media not used as part of a centralized and BTS-approved backup data solution,

D. Defining and auditing compliance with specific retention requirements for permitted storage of cardholder data,

E. Quarterly automatic or manual processes for identifying and securely deleting stored cardholder data that exceed defined retention periods.

1. Payment Account Numbers must be masked when displayed. At all times, the first six and last four digits must be the maximum number of digits displayed.
2. Render Payment Account Numbers unreadable where stored (including on Removable Media, backup systems, and in logs) through one-way hashing, tokenization or encryption.
3. If disk-level encryption is used, rather than file- or column-level database encryption, logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using Authorized User account databases or general network login credentials). Decryption keys must not be associated with user accounts.

Encryption of Data

1. All City Merchant ID (MID) payment cardholder data must be encrypted when transmitted over a public network such as the Internet, and within the City's Trusted Networks. Cardholder data may also appear in the form of the sixteen-digit primary account number plus any of the following: cardholder name, expiration date, or service code.

2. Only necessary data and secure protocols are permitted for City payment card transactions. All other traffic or protocols are explicitly denied in City payment card environments.

Encryption Key Management

1. City Authorized Users are prohibited from knowing or having access to the encryption keys used by the City's PCI Payment Processors or the manufactures of point-of-sale payment devices.

2. Only authorized encryption key custodians are authorized to create, distribute, or maintain City payment card environment encryption keys.

3. All City managed encryption keys must only be created by authorized encryption key custodians using Administrative Accounts and the use of

strong passwords in accordance with **Subsection 5 - IDENTITY AND ACCESS MANAGEMENT.**

4. Knowledge of City managed encryption keys used in payment card environments must be restricted to the fewest number of custodians necessary and be based on business need.

5. Cryptographic keys must be stored in the fewest possible locations.

6. Encryption keys must not be stored or distributed in clear text.

7. All encryption keys must be encrypted with a key-encryption key.

8. Encryption keys must be maintained under a Split Knowledge and Dual Control Regime.

9. City managed encryption keys must be changed at least annually. The keys may be changed more regularly as necessary or as recommended by the associated application or business use care.

10. All compromised encryption keys must be replaced immediately.

11. City managed encryption keys must use BTS and PCI DSS approved algorithms.

12. Encryption key custodians must sign a key custodian form that acknowledges and accepts all encryption key management responsibilities as listed above.

System Development Life Cycle

Payment Card Services System, Application and Service Development

1. Payment processing systems, services and application development must be developed securely in accordance with PCI DSS, based on industry standards and/or industry best security practices for secure coding, and incorporate information security throughout the software development life cycle.

2. Software patches to payment card systems, services and applications must be properly tested before being deployed into a production environment.

3. Test and development environments must be separate from the production environment, with access controls in place to enforce separation.

4. Custom and default application accounts, usernames and passwords must be removed before a payment card system is placed into production.

5. Test and development Authorized Users must employ separation of duties from production environment Authorized Users.

6. Test cardholder data and accounts must be removed before a production system becomes active.

7. Custom software code for payment card processing must be reviewed prior to release to production to identify any potential coding vulnerabilities.

8. Custom software code reviews must be conducted by an individual other than the code author.

9. Production data, such as active primary account numbers, must not to be used for testing and development. Production data must be sanitized before test or development use.

Several OMF Bureau of Revenue and Financial Services' Administrative Rules apply to PCI and payment card process environments:

1. FIN-2.10 - Electronic Payment Processing Services

2. FIN 2.10.01 Guidelines for Electronic Payment Processing Services | Comprehensive Financial Management Procedures

3. FIN 2.10.01 Guidelines for Electronic Payment Processing Services | Comprehensive Financial Management Procedures

4. FIN 2.10.03 Best practices for Processing Payment Card Transactions | Comprehensive Financial Management Procedures

5. FIN 2.10.04 Security of Payment Device Hardware | Comprehensive Financial Management Procedures

Subsection 18 – Information Classification, Protection and Sharing

Purpose

Unauthorized access to City Confidential or Restricted information may introduce fraud, identity theft, or other risks to the City. Because the City's information is stored, processed and shared in both electronic and paper form, safeguards are required to address information classification and protection. The purpose of this policy is to minimize the risks associated with unauthorized access to, abuse, or misuse of City information and to minimize the costs of storing unneeded information.

Administrative Rule

Consistent with federal and state laws, such as the Oregon Revised Statutes relating to public records, the City will protect the information it holds in its custody based on the nature of the information and the risk of unauthorized or undesired access, disclosure, loss or destruction of such information. The degree of protection provided must correlate directly with the risk of exposure, regardless of information media type, storage location, or means of transport.

Information Classification Business System Owners are responsible for the classification of information into one of three categories. These categories allow Authorized Users, Business System Owners, Data Custodians and System Operators to understand the appropriate information handling requirements. Handling is defined to include capture, transmission, storage, retention, and disposal.

Unrestricted - (Public) Information approved for public access. This includes generally available public information, published reference documents (within copyright restrictions), open source material, City website information and press releases. Unrestricted information must still be protected against threats to the integrity of the information.

Restricted - Information which is intended strictly for use within the City. Although most of this information is subject to disclosure laws because of the City's status as a public entity, City information still requires careful management and protection to ensure the integrity and obligations of the City's business operations and compliance requirements. Restricted information includes information associated with internal email systems, City Authorized User account activity and certain personnel information.

Confidential - Information that is legally regulated, sensitive in nature, or requires significant controls and protection. Unauthorized disclosure of Confidential Information could have a serious adverse impact on the City or individuals and organizations who interact with the City. This information includes but is not limited to: 1) cardholder data subject to the Payment Card Industry- Data Security Standard (PCI DSS), 2) personally identifiable information (PII) as defined by the Oregon Consumer Information Protection Act (ORS 646A.600) or the Fair and Accurate Credit Transactions Act of 2003 (also known as the "Red Flag Rules"), 3) Protected Health Information (PHI) as defined by the Health Accountability and Portability Act (HIPAA) and the HI-TECH Act 4) copyrighted, City or third-party trade secrets and 5) attorney-client privileged information. Confidential Information may be subject to public disclosure laws.

Information Protection and Data Loss Prevention

1. **Information Classification** – Information is afforded different protections based on its classification. The chart below summarizes these differences:

City of Portland Information Classification Measures of Protection

Protection Measures	Unrestricted (Public)	Restricted	Confidential

Access Controls	Limited to System Administration	Mandatory	Mandatory
System Maintenance	Mandatory	Mandatory	Mandatory
Logging	Mandatory	Mandatory	Mandatory
Endpoint Detection and Response (EDR) / Anti-Virus-Anti-Malware	Mandatory	Mandatory	Mandatory
Firewalls	Mandatory	Mandatory	Mandatory
Encryption (during Transmission)	No	Recommended	Mandatory
Encryption (Storage)	No	Recommended	Mandatory
Authentication	Limited to System Administration	Mandatory	Mandatory (Strong authentication is required)
Physical Security	Recommended	Mandatory	Mandatory
Data labeling (automated)	Recommended	Mandatory	Mandatory

2. **Data Labels** – Data Custodians and employees processing City Restricted or Confidential Information and media must label information according to their information classification (Unrestricted/Restricted/Confidential).
    a. All electronic media and data must be labeled.
    b. Locations containing information of various levels of classification must be labeled as the most sensitive information contained within the location.
    c. Failure to label documents according to their data classification may result in these documents being treated as public documents and being handled accordingly.
    d. Default labels: If no metadata label is available, filenames can be used to classify data. Please see City of Portland Security Standards 4.0.
3. **Data Loss Prevention** – Data and information storage locations will have limited or restricted access and the location of the data will be modified to reflect their classification level.
    a. Any attempts to share, disclose, copy or exfiltrate any Restricted or Confidential data will be logged, blocked, and reported. This will occur regardless of whether the appropriate data classification label has been applied.

b. All unlabeled documents in Unrestricted locations will be treated as Unrestricted documents and will be handled accordingly. Unlabeled data in Restricted or Confidential locations will be automatically labeled.
c. If data is discovered to be unlabeled or inappropriately labeled it will be relabeled.
d. Business System Owners may prescribe additional measures not illustrated in this rule to classify and protect their information. This rule serves as a baseline classification and protection policy.

4. **Information Sharing** – Information may be shared with external entities and individuals based upon the level of classification. Restricted and Confidential will not be shared without careful review and the authorization to disclose.

Subsection 19 – Cloud Services

Purpose

The information technology industry continues to shift service offerings from on-premises based systems to cloud-based services. The City of Portland is adopting cloud-based services in line with industry trends. Due care and due diligence of City information and Public Records requirements is a mandate of BTS to “ensure confidentiality, integrity and availability of electronic information...”

Administrative Rule

This policy outlines the requirements for Cloud Services use by the City of Portland and is Authorized by the **BTS-2.01 - INFORMATION SECURITY ADMINISTRATIVE RULE**. This policy applies to all City of Portland bureaus, divisions, entities and Authorized Users. Both internal City Cloud deployments (Private Cloud) and external partnerships (Public Cloud) must comply with this policy per City Code, Chapter 3.10 Office of City Attorney | Title 3 Administration3.10.030(B).

Cloud, or 'hosted services' take many forms, including:

IaaS – Infrastructure as a Service – The Cloud Service Provider (CSP) provides the hardware in their data center. The Cloud Consumer manages the configuration and operation of operating systems (such as Windows), databases, storage, applications, security and application use.

PaaS – Platform as a Service – The CSP provides, configures and manages the hardware, operating systems, storage and database platforms. The Cloud Consumer configures and manages the use of the platforms, application’s security and use.

SaaS – Software as a Service – The CSP provides, configures and manages the hardware, operating systems, databases, storage and applications. The Cloud Consumer manages the use of the application and may manage some aspect of application configuration and authorization of user access to the applications.

FaaS – Functions, or applications, as a Service, such as AWS (Amazon Web Services) Lambda, Kubernetes, Docker, etc.

Other - Any other cloud-based service, application, media, platform, or data repository.

Cloud Services

1. Use of Cloud Services must follow all other applicable BTS Administration rules (Technology Services), City Procurement Rules (Chapter 5.33 Goods and Services) and any other applicable City of Portland rules.
    a. Early engagement of BTS Information Security ensures Cloud Services align with applicable regulatory, City information security, privacy, data classification and governance requirements.
2. IaaS and PaaS
    a. For IaaS and PaaS, Bureau of Technology Services (BTS) will manage Azure, Amazon Web Services (AWS) and any other cloud provider infrastructure, platform configuration and Authorized User account access.
    b. Billing for these and other IaaS and PaaS Cloud Services will be managed through BTS. Bureaus will be responsible for monitoring and managing use of metered Cloud Services and associated costs. Billing is the responsibility of the individuals appointed as accountable for each bureau, division, or entity to monitor their data use and billing.
    c. Adjustments to Cloud Service subscriptions will be made through BTS.
3. SaaS and FaaS
    a. Use of and subscription to SaaS/FaaS must be auditable, discoverable, and capable of having information and cyber risk assessed.
    b. Cloud Services providers shall follow all applicable industry control best practices for all critical security updates and patches.
    c. SaaS/FaaS vendors must allow BTS to routinely audit their security posture or provide annual third-party auditor documentation of their security posture, which should be equivalent to a SOC 2 Type II security assessment.
    d. Cloud Services providers are expected to cooperate with City and Law Enforcement investigations of service and data availability, integrity and security, including suspected compromise or breach of data or services.
    e. Non-Standard SaaS or FaaS applications are subject to the BTS Exception Process.

4. Internal and external Cloud Services must leverage the City's Single Sign On (SSO) and Identity and Access Management (IdAM) platforms.
    a. Multi-Factor Authentication must be enabled for access to Cloud Services.
    b. Exceptions will be evaluated during the contracting process.

Legal and Contracts

1. The City's use of Cloud Services must comply with all applicable federal, state, and local laws and regulations.
    a. City Data must be always located within the United States, whether at rest, in transit, or otherwise, except as provided by BTS authorized exception.
2. All contract awards for Cloud Services must comply with City procurement code Chapter 5.33 Goods and Services and Chapter 5.68 Professional, Technical and Expert Service Contracts, as applicable.
3. All contracts for Cloud Services must be submitted to the City Attorney's Office for review and approval as to form, regardless of value as required by Chapter 3.10 Office of City Attorney | Title 3 Administration3.10.030(B).

Data Governance, Privacy and Security

1. Bureaus managing Cloud Services data repositories must align data governance, ownership, privacy and security with City standards and requirements. (See References)
2. Bureaus must comply with City data retention policy and schedules as determined by the City of Portland Auditor's Office.
    a. BTS can assist in configuring compliant IaaS and PaaS services. Also see Exit Strategy below.
3. Cloud Services containing sensitive data types are subject to additional compliance requirements, including but not limited to the following: Payment Card Industry data (PCI), Personally Identifiable Information (PII), Federal Tax Information (FTI), Criminal Justice Information Services data (CJIS), and Personal Health Information (PHI).
4. City-specific data types (Public, Restricted and Confidential) must be stored, accessed and transmitted in accordance with applicable City data governance polices, and as defined in**Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING.**

Exit Strategy

1. Cloud Services and contracts should be developed with an exit strategy for disengaging from the vendor. The City must determine how data can be recovered from the vendor and archived, if necessary, or deleted with confirmation by the vendor, at the time of contract termination or expiration.

Subsection 20 – Software, System and Security Development Lifecycle

Purpose

Information security is a requirement to be considered throughout the System Development Life Cycle (SDLC). This Secure System Development Life Cycle Administrative Rule defines security requirements that must be considered and addressed within every SDLC.

Computer systems and applications are created to address business needs. To do so effectively, system requirements must be identified early and addressed as part of the SDLC. Failure to identify a requirement until late in the process can have major repercussions to the success of a project and result in project delivery delays, deployment of an inadequate system, and even the abandonment of the project. Furthermore, for each phase through which a project passes without identifying and addressing a requirement, the more costly and time-consuming it is to fix problems that occur because of the omission.

Information security must be adequately considered and built into every phase of the SDLC. Failure to identify risks and implement proper controls can result in inadequate security, potentially putting the City at risk of data breaches, reputational exposure, loss of public trust, compromise to systems/networks, financial penalties and legal liability.

Administrative Rule

1. Training. Security is everyone's responsibility and employees require continual training and improvement of skills and knowledge to perform their duties.
2. Define Security Requirements. Information must be classified and protected based on its classification. Adequate security requirements must be defined to protect City Confidential Information and data. A risk assessment early in the system, application or service development process must be conducted to determine requirements. See **Subsection 18 - INFORMATION CLASSIFICATION, PROTECTION AND SHARING.**
3. Design Review. The design must be reviewed iteratively to ensure it complies with City security policies and standards.
4. Develop the Asset. Appropriate security controls must be implemented to mitigate risks that are not avoided, transferred or accepted. Security controls must be justified and documented.
5. Document Baseline Configuration. A configuration baseline provides something to compare against and ensures all similar devices match the baseline.
6. Create Test Data. A process for the development of significant test data must be created for all applications. A test process must be available for applications to perform security and regression testing.
7. Confidential production data should not be used for testing purposes. If production data is used, entities must comply with all applicable

federal, state and external policies and standards regarding the protection and disposal of production data.

8. Test Security Controls. All controls are to be thoroughly tested in pre-production environments that are identical, in as much as feasibly possible, to the corresponding production environment. This includes the hardware, software, system configurations, controls and any other customizations.
9. The testing process, including regression testing, must demonstrate that all security controls have been applied appropriately, implemented correctly and are functioning properly and are countering the threats and vulnerabilities for which they are intended. The testing process must also include vulnerability testing and demonstrate the remediation of critical vulnerabilities prior to placing the system into production.
10. Appropriate separation of duties must be implemented and followed throughout the testing processes such as ensuring that different individuals are responsible for development, quality assurance and accreditation.
11. Secure Code Review. Software code must be reviewed and assessed iteratively both dynamically and statically to ensure compliance with requirements.
12. Deployment and Implementation. Once the software code is deployed it should be penetration tested annually.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Administrative Rules:

BTS Technology Standards Directory

City of Portland Security Standards 4.0 739.21 KB

Glossary | CSRC (nist.gov) – Technology and Information Security terms and definitions

History

Adapted from BTS 2.01-2.19 on December 28, 2022 by Chief Technology Officer

Amended on December 27, 2023 by Chief Technology Officer.

City of Portland Security Standards

Securing Technology is a Universal Responsibility – V4.0

OMF
BTS
Information Security
12/20/2023

Bureau of Technology Services

To deliver strategic leadership through effective, innovative, reliable and secure technology services for our stakeholders.

Table of Contents

PURPOSE

The City of Portland has a fiduciary responsibility to protect technology systems, applications and information entrusted to it by its community members. Therefore, it is necessary to take appropriate measures to ensure the security of these public information technology assets.

INTRODUCTION

To enable the missions of the City of Portland and its bureaus, reduce business risk and technology cost, and protect the City's reputation, it is required that common Information Technology (IT) standards be adopted and implemented on City technology assets. Common standards help ensure a foundational and expected minimal level of security.

The City of Portland Security Standards apply to all City of Portland IT systems and applications, whether City-owned or contractor or vendor-owned systems that process City information, and define the processes, procedures and practices necessary for implementing foundational security throughout the City of Portland. They include specific steps that will be taken to ensure that a secure IT environment is maintained, and all City of Portland systems provide appropriate levels of privacy, confidentiality, integrity and availability.

Responsibly protecting public information technology assets is made possible through an enterprise approach to security that:

(1) Recognizes an interdependent relationship among the Bureau of Technology Services and all partner Bureaus, such that strengthening security for one strengthens all and conversely, weakening one weakens all.
(2) Uses Zero Trust as a guiding principle; assumes mutual security and identity distrust until proven friendly, including relationships and interconnections with government entities, trading partners, and with anonymous users in a least-privilege approach to access control or granting access to City technology resources.
(3) Supports industry security standards and best practices where applicable.

The City of Portland Security Standards complement BTS' "Technology Standards Directory" which defines BTS' standards for a) hardware, devices, and specifications, b) software, applications and their development and integration within the City, c) bureau-centric standards, and d) a sub-set of BTS security standards that are customer facing.

The City of Portland Information Security Standards provides a comprehensive technology security-centric record of standards across BTS' scope of services, including a) Network and Communications Security, b) System Security, c) Data Security, d) Access Control and Identity and Access Management, e) Application Development, f) Technology Security Monitoring, g) Technology Operations Management, g) Cyber Incident Management, and h) Cybersecurity and Risk Management.

SCOPE

The City of Portland Security Standards apply to all City of Portland IT systems and applications, whether City-owned or contractor or vendor-owned systems that process City information.

IT partners throughout the City of Portland are expected to meet these standards. Exceptions must be documented and requested through Bureau of Technology Services Information Security.

ROLES AND RESPONSIBILITIES

The Roles and Responsibility Matrix is designed to guide City of Portland technology staff and agents to appropriate sections of the City of Portland Security Standards. Appropriate sections for review are indicated by a marked checkbox for each role.

Role definitions for purposes of this matrix are:

- Information Security Office – The Information Security Office is the comprised of the Bureau of Technology Services Senior Information Security Officer, currently Christopher Paidhrin, and the staff over which this position sits. The Information Security Office’s primary focuses include information technology risk, governance, compliance and security architecture.
- Business System Owners – Business System Owners play a critical role in the protection of City of Portland information systems. A Business System Owner is generally the most senior authority of an information technology system and is responsible for all aspects of the system and the data it processes and contains.
- Technology System Administrators – Technology System Administrators represent the data custodians and system operators of City of Portland’s information technology systems. Technology System Administrators include any employee or agent that manages an information technology system, including hardware, software, technology services, network infrastructure, communications infrastructure, servers, endpoints, authentication, etc.
- Network Device Administrator – Network Device Administrators are a subset of Technology System Administrators. Network infrastructure is considered an information technology system, but not all Technology System Administrators are responsible for network administration. Network Device Administrators include any employee or agent that manages infrastructure or components related to network or communication.

- Application Developers – Application Developers are responsible for securing custom applications and the systems they run on. Application Developers include any employee or agent involved in coding information technology applications or systems.

The following matrix is designed to help direct roles to specifics areas of this document which may be related to their responsibilities:

City of Portland Security Standards Roles and Responsibilities Matrix	Information Security Office	Business System Owners	Technology System Admins	Network Device Administrators	Application Developers
1.1 Network Segmentation	□	□	☒	☒	□
1.2 Network Device Configuration	□	□	□	☒	□
1.3 Firewall Management	□	□	□	☒	□
1.4 Network Device Administration	□	□	□	☒	□
1.5 Wireless Networks	□	□	□	☒	□
2.1 System Management	□	□	☒	☒	☒
2.2 Secure Configuration	□	□	☒	☒	☒
2.3 Restricted Services	□	□	☒	☒	☒
2.4 System Vulnerability Management	□	☒	☒	☒	☒
2.4.1 Security Patch Management	□	☒	☒	☒	☒
2.5 Protection from Malicious Software	□	□	☒	□	□
2.6 Mobile Computing	□	□	☒	□	□
2.7 Internet of Things (IoT)	□	□	☒	☒	□
3.1 Data Classification	□	☒	☒	□	□
3.2 Data Retention	□	☒	☒	□	□
3.3 Data Loss Prevention	□	□	☒	□	□
3.4 Data Sharing	□	☒	□	□	□
3.5 Data Encryption	□	□	☒	☒	☒

3.5.1	Data Encryption Standards	☐	☐	☒	☒	☒
3.6	Secure Data Transfer	☐	☒	☐	☐	☐
3.7	Digital Certificates	☐	☐	☒	☒	☒
4.1	Access Management	☐	☐	☒	☒	☒
4.1.1	Accounts	☐	☒	☒	☒	☒
4.1.2	Account Auditing	☐	☒	☒	☒	☐
4.2	Password Requirements	☐	☒	☒	☒	☒
4.3	Authentication	☐	☒	☒	☒	☒
4.3.1	User Authentication	☐	☐	☒	☒	☒
4.3.2	Administrator Authentication	☐	☐	☒	☒	☒
4.3.3	Service Account Authentication	☐	☐	☒	☒	☒
4.3.4	External Access Authentication	☐	☐	☒	☒	☐
4.4	Remote Access	☐	☒	☐	☒	☐
4.5	Physical Security	☐	☒	☐	☐	☐
5.1	Application Security	☐	☐	☐	☐	☒
5.2	Secure Coding	☐	☐	☐	☐	☒
5.3	Application Maintenance	☐	☐	☐	☐	☒
5.4	Vulnerability Prevention	☐	☐	☐	☐	☒
5.5	Application Service Providers and Vendors	☐	☒	☒	☐	☒
5.6	Database Security	☐	☐	☒	☐	☒
5.7	Web Services Management	☐	☐	☒	☐	☒
6.1	Security Logs	☒	☐	☒	☒	☒
6.2	Log Collectors	☒	☐	☒	☒	☒
6.3	Security Monitoring	☒	☐	☒	☒	☒
6.4	Intrusion Detection and Prevention	☐	☐	☐	☒	☐

6.5 Security Audits	☒	☒	☐	☐	☐
7.1 Change Management	☐	☒	☒	☒	☒
7.2 Media Handling and Disposal	☐	☐	☒	☐	☐
7.3 Data and Program Backup	☐	☐	☒	☐	☐
7.4 Vendor Management	☐	☒	☐	☐	☐
7.5 Personnel Security	☐	☒	☐	☐	☐
8.1 Incident Response	☒	☒	☒	☒	☒
8.2 Incident Response Plan	☒	☐	☐	☐	☐
9.1 Security Standards	☒	☐	☐	☐	☐
9.2 Security Risk Assessments	☒	☒	☐	☐	☐
9.3 Education and Awareness	☒	☐	☐	☐	☐
9.4 Compliance	☒	☒	☐	☐	☐
9.5 Security Assessments	☒	☒	☐	☐	☐
9.6 Security Program Maintenance	☒	☐	☐	☐	☐

STANDARDS

1. Network and Communications Security

The City of Portland has a responsibility to secure operation of network assets using appropriate layered protections commensurate with City business and cyber risk, and complexity of the technology and service (IT) environment.

1.1 Network Segmentation

Systems and networks must be evaluated by Technology System Administrators and Network Device Administrators. Network segmentation must be used to separate networks with differing security requirements, such as the internet and an internal network that houses City Confidential data.

Network Segmentation Standards:

(1) Logical boundaries are implemented by segmenting networks as determined by system risk, data classification and security requirements.
(2) System risk and approval is documented and submitted to the Information Security Office.
(3) Segmentation controls are enforced to protect segments and individual assets within each segment.

(4) Systems and networks accessible from the Internet or other external networks are segmented from internal networks. External networks are not allowed to directly access internal networks.
(5) By default, access between segmented networks is restricted.

1.2 Network Device Configuration

Network Device Configuration Standards:

(1) Device configurations are standardized and documented.
(2) Deviations from device configuration standards are documented along with the approval.
(3) Internal addresses are masked from exposure on the Internet as necessitated by the risk and complexity of the system.
(4) Controls are implemented to prevent unauthorized computer connections and information flows through methods such as:
    a. Authentication of routing protocols.
    b. Ingress filtering at network edge locations.
    c. Internal route filtering.
    d. Routing protocols are enabled only on necessary interfaces.
    e. Restrict routing updates on access ports.
    f. Secure or disable physical network connections in public areas.

In addition, network devices are considered systems and are subject to standards under Section 2 – System Security.

1.3 Firewall Management

Firewalls and Security Gateway Management Standards:

(1) A stateful firewall is implemented between external and internal networks for network segmentation.
(2) Security zone interfaces are securely segmented from each other and internal networks.
(3) Firewalls and security gateways are configured to:
    a. Allow only secure encrypted protocols for system administration.
    b. Allow administrative access from authorized source IPs or subnets only.
    c. Block services, protocols and ports not specifically allowed or necessary.
    d. Allow only necessary ingress and egress communications between the City of Portland network and segmented security zones.
    e. By default, explicitly deny all traffic not specifically allowed.
    f. Deny incoming and outgoing ICMP traffic at the Internet border except those types and codes relied upon for network diagnostics or other business needs.
    g. Maintain comprehensive audit trails.
    h. Result in a closed state should failure occur.
    i. Operate boundary/perimeter firewalls on a platform specifically dedicated to firewalls.
    j. Send audit and traffic logs to a separate logging system for preservation for at least one year.
    k. Generate logs resulting from the creation and denial of sessions.
(4) Business reason and approval, if necessary, is documented for permitted services, ports and protocols.
(5) Systems are granted access to the internet only when necessary.
(6) Firewalls are managed through a central management system.
(7) Firewall configurations are reviewed at least annually.

(8) Firewall rule sets are reviewed at least every six months.

1.4 Network Device Administration

Network Device Administration Standards:

(1) Use authentication mechanisms commensurate with the level of risk associated with the network segment or device.
(2) Non-console administrative authentication and access is encrypted using technologies such as Secure Shell (SSH), Virtual Private Network (VPN), or Transport Security Layer Security (TLS) for Web-based management and other non-console administrative access.
(3) Simple Network Management Protocol (SNMP) is disabled unless there is a clear business need. If enabled, the vendor defaults are changed.

1.5 Wireless Networks

City of Portland wireless networks are implemented, managed, and maintained by Bureau of Technology Services unless an exception is granted by the Chief Technology Officer or Senior Information Security Officer.

Wireless Device and Network Standards:

(1) Wireless devices connected to the City of Portland network are approved, registered, installed and maintained by the Bureau of Technology Service or authorized delegations for bureau-managed network segments.
(2) Wireless access point connections are securely segmented from the City of Portland network.
(3) Wi-Fi Protected Access (WPA) or its successor for authentication and encryption is used. Use WPA2 Enterprise on all new equipment purchased and existing equipment that supports the protocol.
(4) Wireless vendor defaults, including but not limited to pre-shared keys and passwords, are changed prior to introducing the device to production networks.
(5) A wireless security configuration is documented and enforced across all wireless devices of a specific class.
(6) Rogue wireless devices are continuously monitored for and addressed when presenting a threat to the network.
(7) Open or public access wireless environments do not share assets or traverse infrastructure components that connect to the City of Portland network unless wireless traffic is securely segmented, encapsulated or tunneled over shared infrastructure.

2. System Security

The City of Portland must ensure the secure operation of technology systems using appropriate layered protections commensurate with City business and cyber risk, and complexity of the IT environment.

2.1 System Management

System Management Standards:

(1) Unnecessary functionalities such as scripts, drivers, features, subsystems, file systems and services are disabled.
(2) Configurations are hardened before deployment using hardening standards based on industry best practices such as CIS, NIST, SANS and/or vendor configuration standards and remain hardened throughout the system lifecycle.

(3) Default and initial passwords are changed prior to introduction to the City of Portland network.
(4) An appropriate use banner text is displayed at system access points where initial user logon occurs.
(5) System services and remote communications are disabled where no business need exists.
(6) System configurations are standardized and documented.
(7) Deviations from standard system configurations are documented along with approval.
(8) An inventory of major technology components is maintained within the system environment.
(9) A current list of systems containing Confidential Information is maintained whether it is a City of Portland-owned IT system or contactor/vendor-owned system.
(10)System time is synchronized with central time servers.
(11)System Development Lifecycle (SDLC) governance is maintained for City managed or funded systems, services, endpoints, and interfaces between City and third-party systems and services.

2.2 Secure Configuration

Individual components of technology systems must be configured with a base set of security settings. The secure configuration ensures a base level of expected security on any technology component.

System Secure Configuration Standards:

(1) Each system or class of systems has a documented security configuration.
(2) Secure configurations are based City BTS Administrative Rule requirements and on industry control standards (CIS, NIST, SANS, Microsoft, etc.) or best practices related to the specific system.
(3) Exceptions and deviations are documented along with appropriate approval if necessary.
(4) Secure configurations are reviewed and updated at least annually.
(5) Semi-locked down endpoints (requires review by Information Security)
    a. Where a shared account or generic account is used, further restrictions or compensating controls are required.
    b. If a screen saver exception is granted, it will also include restrictions on the endpoint and all accounts associated with that endpoint.
(6) Kiosk Configuration. Sometimes a customer-facing, or public-facing endpoint is required. These systems must have increased and hardened security measures in place.
    a. Wired network connection only.
    b. USB and all other physical ports should be administratively disabled and physically blocked so that no device can be inserted to the port, except for power and RJ-45/Ethernet.
    c. All radios disabled including Wireless, Bluetooth, NFC, IR, and any other wireless communications.
    d. Restrict Applications to only those necessary using Least Privileges.
    e. Restrict available websites to only those necessary.
    f. A Generic/Shared Kiosk user account with Least Privileges necessary for kiosk function.
    g. Hardware should be secured with a steel cable or locked cabinet.

2.3 Restricted Services

Restricted services are prohibited unless specifically authorized by the Information Security Office. Controls must be implemented to prohibit the use of the following services and applications. The use of restricted services must be documented and approved by the City of Portland Information Security team.

Restricted services include but are not limited to:

(1) Dial-in and dial-out modems.
(2) Peer-to-peer sharing applications.
(3) Tunneling software designed to bypass firewalls and security controls.
(4) Products that provide remote control of technology assets.

2.4 System Vulnerability Management

System Vulnerability Management Standards:

(1) For all systems, a process to identify newly discovered security vulnerabilities is established, such as subscribing to free alert services available on the internet.
(2) Processes that manage the installation and modification of system configuration settings are documented and used.
(3) Only current and supported vendor software releases and equipment are used.

2.4.1 Security Patch Management

Technology System Administrators must develop and document a patch management process commensurate with City business and cyber risk, and complexity of the IT environment.

Security Patch Management Standards:

(1) Responsibilities required for patch management are identified.
(2) Authorized software and information systems deployed in the production environment are identified and inventoried.
(3) Responsible staff are notified with timely patch availability.
(4) Patches are categorized for criticality.
(5) Testing procedures are performed, when required, prior to patch deployment into production environments.
(6) CVSS Score dictates time to patch per the following CVSS 3.0 ratings:

CVSS Category	CVSS Score	Time to Patch
Critical	9.0 – 10	Immediate
High	7.0 - 8.9	14 days
Medium	4.0 - 6.9	30 days
Low	0.1 - 3.9	At next regular patch window
*Exploitable	Any	Immediate

NIST vulnerability metrics may be found here - https://nvd.nist.gov/vuln-metrics/cvss.

(7) Non-compliant systems: Additional security controls may be necessary with systems that do not comply with security patch management standards. Non-compliant systems may be subject to network segmentation, access restrictions, or completely removed from the network. Devices that have not been patched in more than 30 days will be removed from the network at BTS's discretion. The risk evaluation process evaluates individual vulnerabilities as well as the combinations of multiple exploits that may result in compounded vulnerability that can lead to significant attack vectors. Protection from Malicious Software

Protection from Malicious Software Standards:

(1) Anti-malware protection is installed, operating and healthy on all systems commonly affected by malicious software.
(2) Signatures or definitions for anti-malware systems are updated daily.
(3) Malware security actions, warning and notices issued by the Bureau of Technology Services are read and complied with.
(4) All suspected malware incidents or missing/malfunctioning malware protection software is immediately reported to the BTS Helpdesk.
(5) No attempt to circumvent, disable or remove malware protection software, systems or patches is made without prior authorization.
(6) Regular device malware scans are scheduled.
(7) Inbound email is evaluated for malicious content using a secure email gateway or equivalent system.
(8) The Information Security Office performs periodic evaluations to identify and evaluate evolving malware threats to confirm whether operating systems require anti-malware protection.

2.5 Mobile Computing

Examples of mobile devices include laptops, smart phones, network accessible equipment, and portable data storage devices such as zip drives, removable hard drives, and USB data storage devices.

Mobile Computing Standards:

(1) Only Bureau of Technology approved mobile devices may access non-public City of Portland information systems.
(2) Mobile devices unable to support encryption and passwords are protected with a PIN as defined in Section 4.2 – Password Requirements.
(3) Policies and procedures allowing and controlling the use of Confidential Information on mobile devices are documented and implemented.
(4) Confidential Information on mobile devices is encrypted using encryption standards as defined in Section 3.5 – Data Encryption.

2.6 Internet of Things (IoT)

Internet of Things Standards:

(1) IoT devices are appropriately protected from business network traffic through network segmentation as described in Section 1.1 – Network Segmentation.
(2) IoT devices are secured and hardened by applying applicable controls within Section 2 – System Security.

3. Data Security

Data security components outlined in this section are designed to reduce the risk associated with the unauthorized access, disclosure, or destruction of City of Portland data.

3.1 Data Classification

Business System Owners are responsible for the classification of information into one of three categories. These categories allow others to understand appropriate data handling requirements. Handling is defined to include capture, transmission, storage, retention and disposal.

Information is divided into one of three categories based on the sensitivity of the information:

(1) **Unrestricted** (**Public) Information** – Information approved for public access. This information includes public information, published reference documents (within copyright restrictions), open-source material and press releases. This type of information should still be protected against threats to the integrity of the information.

(2) **Restricted Information** – Information which is intended strictly for use within the City. Although most of this information is subject to disclosure laws because of the City's status as a public entity, it still requires careful management and protection to ensure the integrity and obligations of the City's business operations and compliance requirements. This would include information associated with internal email systems, City user account activity information and certain personnel information.

(3) **Confidential Information** – Information that is sensitive in nature requires significant controls and protection. Unauthorized disclosure of this information could have a serious adverse impact on the City or individuals and organizations who interact with the City. This information includes but is not limited to 1) cardholder data subject to the Payment Card Industry - Data Security Standard (PCI DSS), 2) personally identifiable information as defined by the Oregon Identity Theft Protection Act (ORS 646A.600) or the Fair and Accurate Credit Transactions Act of 2003 (also known as the "Red Flag Rules"). This information may be subject to public disclosure laws, 3) Protected Health Information (PHI) as defined by the Health Accountability and Portability Act (HIPAA) and the HI-TECH Act.

3.2 Data Retention

Data Retention Standards:

(1) A data retention policy is documented and maintained, and includes:
   a. Classification of data stored.
   b. Length of time which data must be kept.
   c. Data disposal process.

(2) Data retention policies are aligned with City Archives & Records Management policies and guidelines.

3.3 Data Loss Prevention

Data Loss Prevention Standards:

(1) Where available, technology or controls are implemented to protect against accidental or intentional exfiltration of restricted and confidential information through City of Portland systems.

(2) Classification labels should be applied to all documents and files. If no metadata label is available, then the following filenames are acceptable
   a. [filename]_unrestricted.[extension]
   b. [filename]_restricted.[extension]
   c. [filename]_confidential.[extension]
   d. Example: CreditCardNumbers_confidential.csv

3.4 Data Sharing

When sharing Unrestricted information, follow these guidelines:

(1) Require strong MFA for access – this prevents data being manipulated by bad actors.

(2) Least Permissions – share with as few people as possible to accomplish the goal.

(3) Archive the data when work is complete.

When sharing Confidential or Restricted Information outside the City of Portland, an agreement must be in place unless otherwise prescribed by law. The agreement (such as a contract, a service level agreement, Business Associate Agreement (HIPAA), or a dedicated data sharing agreement) must address the following:

(1) The information that will be shared.
(2) The specific authority for sharing the information.
(3) The classification of the information shared.
(4) Access methods for the shared information.
(5) Authorized users and operations permitted.
(6) Protection of the information in transport and at rest.
(7) Storage and disposal of information no longer required.
(8) Backup requirements for the information if applicable.
(9) Other applicable information handling requirements.

3.5 Data Encryption

Encryption technologies are used to prevent unauthorized individuals from reading or altering confidential or sensitive information stored on City systems and network resources or transmitted across City and public networks.

The storage and transmission of Confidential Information on the City of Portland network must be implemented using industry standard algorithms validated by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program. Encryption must be applied in such a way that it renders data unusable to anyone but authorized personnel, and the confidential process, encryption key or other means to decipher the information is protected from unauthorized access.

The following examples of data and information are encrypted:

(1) Criminal justice data (CJI) when transmitted across public networks or any private network that is shared with non-criminal justice users.
(2) User or application level credentials (account names & passwords).
(3) Payment Cardholder Data (PCI) including primary account number, cardholder name, expiration date, and service code.
(4) Personally identifiable information (PII) as defined by the Oregon Identity Theft Protection Act.
(5) Electronic protected health information (ePHI) such as health benefit data covered under HIPAA privacy regulations.
(6) Any 802.11 wireless or Remote Network Access communications when used to connect to the City's networks or computing resources.
(7) Confidential data stored on portable computing devices such as laptops, smartphones, and USB thumb drives.

Note: This is not a complete list and is provided to give general guidance on commonly used confidential/sensitive information subject to higher levels of protection. Please contact the Information Security Office for appropriate classification of data and to help determine if encryption is required.

BTS-2.18 - Information Classification & Protection (Administrative Rule) provides minimum requirements for the protection of City information.

3.5.1 Data Encryption Standards

Proven, standard algorithms shall be used as the basis for encryption technologies. Symmetric cryptosystem key lengths must be at least 128 bits. The Information Security Office will periodically review City encryption key length requirements and upgrade them as technology allows.

(1) Use the following encryption protocols; TLS 1.2, or higher. SSLv2, SSLv3, TLS 1.0, and TLS 1.1 are deprecated protocols and are prohibited.
(2) Use the following digital signature algorithms; RSA, DHE (2048+ bits), ECDHE.
(3) Use the following encryption algorithms; AES-128, AES-256. RC4 and 3DES-168 are deprecated algorithms and are prohibited.
(4) Use the following hashing algorithm; SHA2 or better. MD5 and SHA1 are deprecated algorithms and are prohibited.
(5) VPN Encryption Standards

Setting	**Value** **Recommended in green** Allowed in black
P1 IKE version	**IKEv2**
P1 Proposal	AES-GCM (best performance), AES-CTR, AES-CBC, AES-CCM with 128/192/256 key
P1 Auth Method	Certificate (internal) Pre-shared secret key (PSK)
P1 Auth	SHA512 SHA384 SHA256
P1 Diffie-Hellman Groups	**14, 15, 16, 17, 18, 19, 20, 21**
P1 Key Life	24 hours
P2 Mode	IPsec-v3

P2 Encryption	AES-GCM (best performance), AES-CTR, AES-CBC, AES-CCM with 128/192/256 key
P2 Authentication	SHA256,384,512, AES-GMAC
P2 Key Life	8 hours
Perfect Forward Secrecy	**Same as or stronger than IKE DH** when resources allow

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Chief Technology Officer or the Senior Information Security Officer.

3.6 Secure Data Transfer

Business System Owners must ensure appropriate protection of information transmitted electronically.

Secure Data Transfer Standards:

(1) All manipulations or transmissions of information during the exchange are secure.
(2) If intercepted during transmission the information cannot be deciphered.
(3) When necessary, confirmation is received when the intended recipient receives the information.
(4) Systems use encryption per Section 3.5 – Data Encryption.
(5) For systems not on the City of Portland network, this standard applies when transmitting Confidential Information outside of the City of Portland network.

3.7 Digital Certificates

Digital certificates can be used to provide integrity and confidentiality when used during data exchanges.

Digital Certificate Standards:

(1) Digital certificates are issued and managed through a standardized enterprise process.
(2) Digital certificates can be revoked in a timely manner.
(3) Self-signed certificates are replaced with certificates from an authorized certificate authority.

4. Access Control, Identity and Access Management

4.1 Access Management

Access controls must confirm to the principle of least privilege, meaning system access is limited to the minimum privileges required to perform required functions.

Access Management Standards:

(1) Access to data, application and system functions is only allowed for users and support personnel who have a business need for such access.

(2) The principles of least privilege and need to know are practiced when determining access requirements for an account.
(3) Authentication and authorization controls are appropriately robust for the risk of the application or system to prevent unauthorized access.
(4) Access rights of users to information and information processing facilities are removed upon suspected compromise, termination of their employment or contract, or are adjusted upon change in status.
(5) The use of programs or utilities capable of overriding system and application controls are restricted.

4.1.1 Accounts

Account Standards:

(1) A formal procedure for issuance, management and maintenance of UserIDs and passwords is documented and established.
(2) Each user is issued a unique user account and password.
(3) The use of group, shared, or generic UserIDs/passwords are prohibited without authorization.
(4) User accounts found to be inactive for a period of 90 days are disabled.
(5) User accounts that have been disabled for a period greater than 1 year are deleted.
(6) Accounts are managed through centralized enterprise account technologies (i.e. Active Directory, ADFS) when the technology allows.
(7) Local accounts are prohibited unless documented with business justification and appropriate approval.
(8) The addition, deletion, and modification of UserIDs, credentials, and other identifier objects is controlled.
(9) User identity is verified before performing password resets.
(10) First-time passwords are set to a unique value per user that must be changed immediately after first use.
(11) A lockout policy is implemented which meets or exceeds:
    a. Maximum of six incorrect login attempts before account lockout, and,
    b. Account lockout period of a minimum of 30 minutes or until reset by an administrator.
(12) Accounts used by vendors for remote maintenance are enabled only during the time needed.

4.1.2 Account Auditing

Accounts and access policies must be reviewed for effectiveness to ensure continued protection.

Account Auditing Standards:

(1) User access rights are periodically reviewed using a formal process, and based on risk to the data, application, system, device or service, which may be cloud hosted by a third party.
(2) Mechanisms to monitor the use of privileges are implemented.

4.2 Password Requirements

Password Requirements Standards:

(1) Password administration rules must be technically or procedurally enforced.
(2) UserID/password combinations are considered Confidential Information and must be protected.
(3) Passwords must not repeat a previously used password within the last 10 password change events.

(4) Service or shared account passwords are changed immediately when an employee with knowledge of the password separates from employment or is reassigned to responsibilities in which such knowledge is no longer required.

(5) Password strength requirements are determined by account category and authorized levels of access. The City currently has three categories of accounts: Authorized User Accounts, Administrative Accounts, and Service Accounts. Each account category has different trust levels with different requirements.

a. Authorized User Accounts: 12 character minimum, no password complexity, 24 month password expiration when Multi-Factor Authentication (MFA) is enabled.

b. Administrative Accounts: 15 character minimum, 3 of 4 character types, 90 day password expiration.

c. Service Accounts: 20 character minimum, randomly generated, all 4 character types, 24 month password expiration.

Passwords must:

d. Be a minimum of 8 characters long. 20 characters is recommended for high security.

e. Contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters, as supported by the service.

f. Not contain the user’s name, UserID or any form of a full name.

g. Not consist of a single complete dictionary word but can include a passphrase.

h. Be significantly different from the previous four passwords. Passwords that increment (Password1, Password2, Password3 ...) or follow an easily predictable pattern (Spring2019, Summer2019, Fall2019 …) are not considered significantly different.

i. Meet all applicable requirements and can include a passphrase of dictionary words.

(6) PIN or pass codes must:

a. Be a minimum of six numeric characters or six alpha-numeric characters when the service supports mixed characters.

b. Not contain more than a three consecutive character run. Pass codes consisting of 12345a, abcde1 are not acceptable.

c. Render the device unusable after 10 failed login attempts.

(7) Passwords are not inserted into email messages and other forms of electronic communication. Leaving a temporary use password as a message on a user’s confirmed voicemail is acceptable, however care must be taken to make sure such passwords are not overheard by anyone other than the intended recipient.

4.3 Authentication

Authentication is used to validate the identity of users performing functions on systems. Selecting the appropriate authentication method is based on risks to information and data.

Authentication Standards:

(1) Account authentication to systems meets the controls appropriate for the type of authentication.

(2) Users are identified with a unique identifier, for their individual use only, before allowing them to access components, systems, networks, or data.

(3) An appropriate use banner text is displayed at system access points where initial user logon occurs.

(4) Where supported, all systems require a user to re-authenticate to re-active idle sessions after 15 minutes of keyboard or mouse inactivity.

(5) Authentication occurs using existing City of Portland's SAML/SSO capabilities where technically possible.
(6) Modern Authentication is required for User Accounts which is managed by BTS Account Administrators.

There are three basic types of accounts:

(1) User Accounts – User accounts are used interactively to authenticate with systems. User accounts are used for general, non-administrator system access.
(2) Administrator Accounts – Administrator accounts are used interactively to authenticate with systems to gain privileged administrator access. These accounts must be separate from general user accounts to reduce risk of credential exposure and account compromise.
(3) Service Accounts – Service accounts are non-user accounts used by a system for service, daemon or application execution. They are not used interactively, meaning service accounts are intended to be used programmatically only and not used for manual logins.

4.3.1 User Authentication

User Authentication Standards:

(1) A UserID and hardened password as defined in Section 4.2 – Password Requirements is required.
(2) Password expiration period not to exceed 90 days unless an exception is approved by the Chief Technology Officer and Senior Information Security Officer.

4.3.2 Administrator Authentication

Administrator Authentication Standards:

(1) A UserID and hardened password as defined in Section 4.2 – Password Requirements is required
(2) Password expiration period not to exceed 90 days.
(3) A discrete account used only for interactive system administration functions is required.
(4) Administrator account password is different than all other accounts.

Administrator passwords are recommended to be at least 15 characters in length.

Multi-factor authentication is recommended for administrator authentication to safeguard against unauthorized privileged access. Multi-factor authentication may consist of tokens, certificates, one-time passwords, or other method of authentication outside of "something the user knows".

4.3.3 Service Account Authentication

Service Account Authentication Standards:

(1) Documentation of purpose and period of use is required.
(2) A discrete account used only for the defined privileged functions is required, and never used by an individual.
(3) A hardened password as defined in Section 4.2 – Password Requirements is required with an extended password length of 15 characters.

Service account passwords are recommended to be changed at least once every two years.

4.3.4 External Access Authentication

Authentication to the City of Portland network and data from locations outside the City of Portland network may require additional security controls. Services requiring additional authentication controls include the City of Portland's Remote Access platform and Office 365 tenant.

In addition to account authentication controls in 4.3.1, accounts accessing the City of Portland's remote access platform and Office 365 tenant must be configured to:

(1) Require multi-factor authentication.

Multi-factor authentication may consist of tokens, certificates, one-time passwords, or other method of authentication outside of "something the user knows".

4.4 Remote Access

Remote network access to City of Portland networks from external networks must occur only via Bureau of Technology Services maintained virtual private network (VPN) systems or firewalls.

Remote Access Standards:

(1) Multi-factor authentication is required.
(2) Industry standard protocols are used for remote access solutions.
(3) Remote access solutions prompt for re-authentication or performs automated session termination after 30 minutes of inactivity.
(4) Full VPN access is available to Bureau of Technology Services maintained systems only.
(5) Non-City of Portland devices are restricted to indirect network access only.
(6) Split-tunneling is not permitted.

Multi-factor authentication may consist of tokens, certificates, one-time passwords, or other method of authentication outside of "something the user knows".

4.5 Physical Security

Business System Owners must ensure adequate physical security and environmental protections are in place to maintain the confidentiality, integrity, and availability of the computer systems within the Business System Owner's control. Business System Owners must prevent unauthorized access, damage, or compromise of information technology assets. Investments in physical and environmental security must be commensurate with the risks, threats, and vulnerabilities unique to each physical site and location.

At a minimum, the following physical security measures and objectives must be implemented where applicable to protect City of Portland technology assets and sensitive information:

(1) Mainframes, servers, network equipment, desktops, laptops, mobile devices, and removable media containing sensitive data and other essential computer and network devices shall be stored in a secure location, such as a locked room, that protects them from unauthorized physical access, use, misuse, destruction or theft of physical protection and guidelines for working in secure areas.
(2) Smoke/fire alarm and suppression systems are required for all data centers, server rooms and telecommunication closets to mitigate personnel harm and/or damage to City assets in the event of a fire.

(3) Temperature and ventilation control measures are required for all data centers and server rooms to protect City assets from preventable service disruptions or physical harm from environmental conditions.
(4) All mission critical data centers must employ emergency power control systems (backup generators and uninterruptible power supplies) to avoid disruptions and/or equipment/data harm due to power related failures.
(5) Inventory control measures such as inventory reports, asset tags or other identification markings for tracking are required per City accounting policy.
(6) All access to restricted areas, such as data centers, server rooms, and telecommunications closets, by unauthorized individuals must always be conducted with an authorized City employee escort.
(7) Access keys and key codes to restricted areas must be limited to only those individuals needing entry to fulfill their job responsibilities. Records of individuals' assigned access must be maintained.
(8) All specific tools, systems, or procedures implemented to meet physical security requirements must be selected based on importance to safety, security and compliance with City policies and standards.

5. Application Development

5.1 Application Security

Application Security Standards:

(1) Applications provide for data input validation to ensure the data is correct and appropriate and cannot be used to compromise security of the application, technology infrastructure, or data.
(2) Procedures are in place to manage the installation of applications on operational systems including but not limited to servers and endpoints.
(3) Access to program source code is restricted to only those individuals whose job requires such access.
(4) Specific requirements are included in contracts for outsourced software development to protect the integrity and confidentiality of application source code.
(5) Implementation of changes will be managed using formal change management procedures.
(6) Appropriate access and security controls, audit trails, and logs for data entry and data processing exist.
(7) Appropriate data protection requirements are met.
(8) If account credentials are stored, passwords are encrypted, and are not stored in plain text or encoded.
(9) Application components are inventoried, and vulnerabilities are managed per Section 2.4 – System Vulnerability Management.
(10)Software Development Lifecycle (SDLC) governance is maintained for City managed or funded applications, services, software and computer code.

5.2 Secure Coding

Application Developers must develop software applications based on industry best practices and include information security throughout the software development life cycle, including the following:

(1) Separate development, test, and production environments.
(2) Implement separation of duties or other security controls between development, test and production environments. The controls must reduce the risk of unauthorized activity or changes

to production systems or data including but not limited to the data accessible by a single individual.

(3) Production data used for development testing must not compromise privacy or confidentiality. Prohibit the use of Confidential Information in development environments unless specifically authorized by the City of Portland's Information Security Office. Production data in any environment must meet or exceed the level of protection required by its data classification.
(4) Removal of test data and accounts before production systems become live.
(5) Removal of custom application accounts, usernames, and passwords from production environments before applications become active or are released to customers.
(6) Review of custom code prior to release to production or customers to identify potential coding vulnerabilities as described in Section 7.4 – Vulnerability Prevention.
(7) Appropriate placement of data and applications in the technology infrastructure based on the risk and complexity of the system.
(8) Use of appropriate authentication levels.
(9) Software Development Lifecycle (SDLC) governance is maintained for City managed or funded technology coding.

5.3 Application Maintenance

Application Maintenance Standards:

(1) System changes are reviewed and tested to ensure there are no adverse impacts on operations or security.
(2) Obtain timely information about technical vulnerabilities of information systems being used, evaluate the City's exposure to such vulnerabilities, and take appropriate measures to address the associated risk.

5.4 Vulnerability Prevention

Application Developers must prevent common coding vulnerabilities in software development processes. Application Developers must:

(1) Develop software and applications based on secure coding guidelines. An example is the Open Web Application Security Project guidelines. See www.owasp.org – "The Ten Most Critical Web Application Security Vulnerabilities" which include:
    a. Un-validated input.
    b. Weak or broken access control such as malicious use of UserIDs.
    c. Broken authentication/session management such as use of account credentials and session cookies.
    d. Cross-site scripting (XSS) vulnerabilities.
    e. Buffer overflows.
    f. Injection flaws such as SQL injection.
    g. Improper error handling that creates other conditions, divulges system architecture or configuration information.
    h. Insecure storage.
    i. Denial of service.
    j. Insecure configuration management.
(2) Review code to detect and mitigate code vulnerabilities that may have security implications when significant changes have been made to the application.

5.5 Application Service Providers and Vendors

Applications and cloud-based services hosted by an Applications Service Provider or other third party outside of the shared, trusted environment must comply with:

(1) Applicable City of Portland Security Standards and standard contract language for cloud-hosted services which includes the following references to BTS Administrative Rules.

“To the extent required by law and as applicable, Contractor shall comply with City of Portland, Bureau of Technology Services Information Security Administrative Rules 2.01, 2.02, 2.08, 2.12 and 2.15 and 2.19. These rules are located at: http://www.portlandonline.com/auditor/index.cfm?c=26821."

The operation of such applications must not jeopardize the City’s technology security environment or cyber risk posture.

5.6 Database Security

To maintain the security of the City of Portland’s internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program’s source code in clear text.

Database Security Standards:

(1) Database user and system account access utilize principles of least privilege.
(2) Database user and system accounts are not granted sysadmin privileges.
(3) Database service account passwords must comply with password and authentication controls in Sections 4.1.1 - Accounts, 4.2 – Password Requirements and 4.3 - Authentication.
(4) Database credentials are protected from unauthorized parties when stored within executing code or stored in a separate file leveraging encryption or other secure method.
(5) Database credentials are not stored in a location that can accessed externally through a web browser.
(6) Databases serving externally facing web services are segmented from Internet serving networks as well as from the City of Portland internal network.

5.7 Web Services Management

Web Services Management Standards:

(1) A secure configuration is documented and implemented (Section 2.2 – Secure Configuration).
(2) Appropriate encryption is used where applicable (Section 3.5 – Data Encryption).
(3) Appropriate authentication and access controls are in place where applicable (Section 4 – Access Control, Identity and Access Management).
(4) Default web service pages are made unavailable or are replaced.
(5) Self-signed certificates are replaced with certificates from an authorized certificate authority. (Section 3.7 – Digital Certificates)

6. Security Monitoring and Testing

Audit logs recording user activities, exceptions, and information security events are necessary to detect and audit unauthorized information processing activities.

6.1 Security Logs

A logging strategy is necessary that addresses each system based on City business and cyber risk, and the complexity of the system.

Security Logs Standards:

(1) Logs are generated for events, exceptions and user activities necessary to reconstruct unauthorized activities defined by the strategy.
(2) Logs are retained for a minimum of one year.

Where technology allows, these events are the minimum types of events which are logged:

(1) Successful and unsuccessful logon events.
(2) Successful logoff events.
(3) Successful and unsuccessful modify authentication policy events.
(4) Successful and unsuccessful modify user account, security group, or permission events.
(5) Successful and unsuccessful audit policy change events.
(6) Successful and unsuccessful attempts to access, modify, or delete audit log files.
(7) Events generated by security functions (for example, firewalls, intrusion prevention systems, authentication systems, etc.).

Additional logging requirements may be necessary to meet specific compliance frameworks (CJIS, etc.).

6.2 Log Collectors

Log collectors are systems designed to receive logs from other systems. Sending logs to a separate centralized system provides security and helps log correlation and troubleshooting.

Log Collector Standards:

(1) Stored logs are protected against tampering and unauthorized access.
(2) System time is synchronized with central time servers.
(3) Logs are retained for a minimum of one year, 7 years for FTI or as required by compliance domains.

6.3 Security Monitoring

Security Monitoring Standards:

(1) System audit logs are reviewed periodically commensurate with system risk and data classification.
(2) Security incidents and suspected security events are immediately reported to Bureau of Technology Services or the Information Security Office through a BTS HelpDesk phone call or service ticket.

6.4 Intrusion Detection and Prevention

Bureau of Technology Services monitors networks, devices, access, and activities with Intrusion Detection and Prevention systems. Intrusion Detection and Prevention systems must be configured to log information continuously and logs reviewed periodically.

Intrusion Detection and Prevention Standards:

(1) Critical networks are evaluated for intrusion detection or prevention systems.

(2) Signatures or definitions for intrusion detection and prevention systems are updated daily.
(3) System and audit logs are retained for at least one year.
(4) Alarm and alert functions are enabled and sent to appropriate response staff.
(5) Logs are reviewed regularly by system operators.
(6) Suspected and/or confirmed instances of successful and/or attempted intrusions are immediately reported to Bureau of Technology Services or the Information Security Office.

6.5 Security Audits

Information Security Assessments must be conducted periodically to review and assess the effectiveness of existing cybersecurity physical controls related to Citywide technology services. These assessments include testing of cyber and physical security controls to make sure unauthorized access attempts can be identified and prevented or stopped. Examples of periodic testing include penetration tests, vulnerability assessments and system code analysis.

The Information Security Office may perform information security audits that include:

(1) Performing vulnerability scanning on City of Portland network assets regularly.
(2) Periodic penetration testing as documented by Information Security processes.
(3) Periodic password testing.

The Information Security Office must be informed when security audits are performed on City of Portland networks by other staff or third parties.

7. Operations Management

7.1 Change Management

Bureau of Technology Services Change Management provides a systematic approach to managing all changes made to a service or system, with the purpose of reducing City business and cyber risk, downtime, and increasing communication and productivity.

Bureau of Technology Services Change Management

Change Management Standards:

(1) Changes to City of Portland information technology systems must go through an established change management process.
(2) Changes are documented and include:
    a. Change Impact
    b. Change approval by authorized parties
    c. Functionality testing to verity the change does not adversely impact the security of the system
    d. Back-out procedures.

7.2 Media Handling and Disposal

Media Handling and Disposal Standards:

(1) Storage media that is owned, leased or otherwise under the physical control of the City of Portland is sanitized securely and safely when no longer required, using formal, documented procedures.
    a. Equipment containing storage media is sanitized prior to disposal, consistent with NIST SP 800-88 Guidelines for Media Sanitation.

   b. All data and software are destroyed, securely overwritten or otherwise made unavailable consistent with software licensing agreements.
   c. Media is verified as fully sanitized.
   d. Sanitization tools are tested and maintained per a documented schedule.
   e. Records are maintained that provide the date and methods used to sanitize and/or dispose of the storage media and include attestation of the process by at least one individual.
   f. Media is physically destroyed when it cannot be sanitized using software tools. Media may be physically destroyed even when the software sanitization tools are effective. Physical destruction may be accomplished by shredding, pulverization or other means that ensure the media can never be re-used. Disposal of physically destroyed media should be conducted in an environmentally responsible way.

(2) Staff responsible for data disposal are trained to perform and attest to media sanitization functions.
(3) Media sanitization and disposal documentation is protected against unauthorized access.
(4) Media containing information is protected against unauthorized access, misuse, or corruption from the time it is removed from operational status to the time it is sanitized or disposed.

7.3 Data and Program Backup

Data and Program Backup Standards:

(1) Data archival and rotational requirements for backup media are satisfied.
(2) Procedures for periodic tests to restore system data from backup media are documented and implemented.
(3) Recovery procedures for critical systems are tested.
(4) Methods to secure backup media are established.
(5) Media backups are stored in a secure location such as a designated temporary staging area, an off-site facility, or a commercial storage facility.

7.4 Vendor Management

Vendor Management Standards:

(1) Appropriate language is included in vendor contracts to require compliance with City of Portland administrative rules, policies, standards, compliance frameworks, and requirements as referenced in Section 5.5 Application Service Providers and Vendors.

7.5 Personnel Security

Personnel Security controls are designed to reduce risks of human error, theft, fraud, or misuse of facilities. They help Business System Owners ensure that users are aware of information security threats and are equipped to support the City of Portland security policy during their normal work.

Personnel Security Standards:

(1) Information Security orientation is provided to employees and contractors who have access to City of Portland information technology assets.
(2) Reference checks and background investigations are conducted as required by information technology compliance frameworks and as aligned with OMF Human Resources guidelines.
(3) Employees receive the general information security awareness education as described in Section 9.3 – Education and Awareness at least annually.
(4) Appropriate sanctions are imposed for security violations.

(5) Processes are established for the timely removal of system access for employees and contractors when duties change or when separating from service.

(6) Employees and contractors are required to comply with these City of Portland Security Standards and Bureau of Technology Administrative Rules. Each user should be made clearly aware of this responsibility.

8. Incident Management

8.1 Incident Response

Incident Response is a shared responsibility for all roles involved with technology. If an incident is suspected, report the incident immediately to the Bureau of Technology Services or the Information Security Office through a BTS HelpDesk phone call or service ticket.

8.2 Incident Response Plan

Incident Response Plan Standards:

(1) An Incident Response Plan will be documented and distributed to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, roles and responsibilities, and communication and contact strategies in addition to the following:

   a. Escalation procedures.
   b. Designate specific personnel to respond to alerts.
   c. Responsible roles are prepared to implement the incident response plan and to respond immediately to a system breach.
   d. Provide appropriate training to staff with security breach response responsibilities.
   e. Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
   f. Incorporate the incident response plan in the City of Portland Security Program.

(2) The incident response plan is tested at least annually.

9. Security and Risk Management

9.1 Standards Document

The Information Security Office is responsible for the maintenance of these City of Portland Security Standards.

Standards Document Standards:

(1) Content is aligned with City of Portland information technology risk management strategies.

(2) Content is adjusted as deemed necessary through risk evaluation of industry trends and best practices, threats and business needs.

(3) Content is reviewed and updated at least annually.

The City of Portland Security Standards are available at [insert link].

9.2 Security Risk Assessments

The Information Security Office has a risk assessment process designed to identify compliance, technology and/or business risks within the scope of the assessment.

Risk assessments are designed to:

(1) Identify risk within the scope of the assessment.
(2) Identify potential threats to in-scope assets.
(1) Identify vulnerabilities that might be exploited by the threats.
(2) Identify impacts to confidentiality, integrity, and availability of services or data identified as within scope.
(3) Assess the likelihood that security failures may occur based on prevailing threats and vulnerabilities.
(4) Consider business, legal, regulatory requirements, and/or contractual security obligations.

Contact the Information Security Office to request or inquire about information technology risk assessments.

9.3 Education and Awareness

A Security Education and Awareness program must be maintained by the Information Security Office. Security awareness training is the formal process of educating City of Portland system users about computer and data security.

Education and Awareness Standards:

(1) The process includes annual content review and content refresh as necessary to keep the material current and relevant.
(2) All employees are required to receive annual security awareness training that includes the risks of data compromise, their role in data loss prevention, and how to respond in the event of an incident as relevant to the individual's job function.

9.4 Compliance

The City of Portland maintains information and data which must comply with data security standards from third-party compliance frameworks. These frameworks include but are not limited to Payment Card Industry (PCI) – Data Security Standard, Health Insurance Portability and Accountability Act (HIPAA) guidelines and the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.

Compliance Standards:

(1) The Information Security Office is engaged during planning stages of projects and systems with relevant shared scope to compliance frameworks.
(2) Systems, services and technologies where compliance frameworks have jurisdiction are compliant when implemented and remain compliant during the technology's lifecycle.
(3) Vendors and contractors are required to maintain compliance to these City of Portland Security Standards and applicable compliance framework data security standards.
(4) Instances of non-compliance are documented and reported to the Information Security Office.

9.5 Security Assessments

The Information Security Office will use the City of Portland Security Standards, and applicable compliance frameworks, when assessing system security. Assessments may be initiated by the Information Security Office by identifying services based on security and data risk and may be requested by City of Portland Business Owners.

Security Assessments Standards:

(1) Assessments are designed to be productive, efficient and identify security gaps within a City of Portland system.
(2) Support is given to assessors and assessments to facilitate a complete assessment.
(3) Reports are generated from assessments, and the reports are distributed to appropriate individuals, including the Business Owner and Bureau of Technology Services leadership.

9.6 Security Program Maintenance

Security Program Maintenance Standards:

(1) Processes and documentation within the Information Security Program are reviewed and updated at least annually.
(2) Areas to improve effectiveness of the Information Security Program are identified and implemented.

EXCEPTIONS

Where the City of Portland Security Standards apply but systems are not able to comply, exceptions may be granted. Exceptions to Security Standards may only be granted through the Information Security Office.

Exception requests must include:

(1) The control or controls with which a system cannot comply.
(2) Business reason as to why a system cannot comply.
(3) Length of time the exception is necessary.
(4) Approval from Business System Owner or Bureau Director.
(5) Remediation plan summarizing plan to comply.

In some cases, compensating controls may be necessary to mitigate risk. A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement.

DEFINITIONS

Definitions within BTS Admin Rules and Standards are sourced from the National Institute of Standards and Technology. A link to the NIST definitions glossary is provided here.

Glossary | CSRC (nist.gov) – Technology and Information Security terms and definitions

Common Usage Terms with simplified definitions:

Access – The ability to use, modify, or affect an information technology system or to gain entry to a physical area or location.

Application – A computer program or set of programs that meet a defined set of business needs.

Asset – Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology system, data, networks, circuits, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

City of Portland Network – The shared, internal enterprise network bounded by a security layer defined by firewalls, proxy servers, security appliances, secure gateways and other Bureau of Technology Services managed security services.

Contractor – The firm, its employees and affiliated agents. Contractor also includes any firm, provider, organization, individual, or other entity performing the business activities on behalf of the City of Portland. It will also include any subcontractor retained by Contractor as permitted under the terms of the Contract. Contractor and third-party are synonymous as defined within the Definitions section of this standard.

Demilitarized Zone (DMZ) – An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.

Environmental Security – Physical protection against damage from fire, flood, wind, earthquake, explosion, civil unrest and other forms of natural and man-made risk.

Firewall – An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the City of Portland. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Infrastructure – Infrastructure consists of the equipment, systems, software, and services used in common across an organization, regardless of mission/program/project. Infrastructure also serves as the foundation upon which mission/program/project-specific systems and capabilities are built.

Common capabilities examples include information technology security systems, servers, routers, endpoints, networked Supervisory Control and Data Acquisition (SCADA) systems, and networked printers (multifunction devices).

Internal System or Network – A system or network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (regarding confidentiality and integrity).

Intrusion Detection Systems (IDS) – A security service that monitors and analyzes network or system events for finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Prevention Systems (IPS) – A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Malware – Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Mobile Device – A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.

Multi-factor Authentication (MFA) – An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Network – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Device – Network devices are components used to connect computers or other electronic devices together so that they scan share resources.

Password – A string of characters (letters, numbers and other symbols) that are used to authenticate an identity or to verify access authorization. A passphrase is a special case of a password that is a sequence of words or other text. In this document, the use of the term “password' includes this special case.

Penetration Test – A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations.

Risk Assessment – The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

Risk Management – The on-going process of assessing the risk to information technology resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Security – Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

Security Control – A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

A system may include, but is not limited to:

(1) Applications
(2) All data associated with the system regardless of source or where it resides.
(3) End-user authentication systems.
(4) Hardware (voice, video, radio transmitters and receivers, network equipment, mainframes, servers, workstations, personal computers, laptops, and all endpoint equipment).
(5) Software (operating systems, application software, middleware, microcode).
(6) Information technology infrastructure (networks, connections, pathways, servers, wireless endpoints).
(7) Services (data processing, telecommunications, office automation, and computerized information systems).
(8) Telecommunications hardware, software, and networks.
(9) Intelligent control systems such as video surveillance, HVAC, and physical security.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Token – Something that a claimant possesses and controls (such as a key or password) that is used to authenticate a claim. For use in multi-factor authentication.

Virtual Private Network (VPN) – A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.

Vulnerability – A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerability Assessment – Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

REVISION HISTORY

December 20, 2023 – Technical Standards Update – Christopher Paidhrin
November 2, 2022 – Annual Review – IS Team
October 28, 2021 –Annual review – IS Team
July 1, 2020 – Annual review – Christopher Paidhrin
July 1, 2019 – Initial effective date – Christopher Paidhrin

February 1, 2019 – Policy adopted – Christopher Paidhrin
April 15, 2019 – Information Security Peer Review – Josh Scott, Edith Brown
March 11, 2019 – Initial review – Christopher Paidhrin
February 7, 2019 – Initial draft – Dean Musson

CONTACT INFORMATION

For questions about this policy, please contact the Information Security Office.

APPROVING AUTHORITY

Jeff Baer – Chief Technology Officer, Bureau of Technology Services
Elyse Rosenberg – Deputy Chief Technology Officer, Bureau of Technology Services
Christopher Paidhrin – Senior Information Security Officer, Bureau of Technology Services

REFERENCES

National Institute of Standards and Technology (NIST) Glossary National Institute of Standards and Technology (NIST) Special Publication 800-41 – Guidelines on Firewalls and Firewall Policy

National Institute of Standards and Technology (NIST) Special Publication 800-53 – Security and Privacy Controls for Information Systems and Organizations

Open Web Application Security Project – www.owasp.org

Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures

U.S. Department of Justice – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy

Washington State Office of the Chief Information Officer – Securing Information Technology Assets Standards