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 5
INTRODUCTION 5
SCOPE 6
ROLES AND RESPONSIBILITES 6
STANDARDS 9
1. Network and Communications Security 9
1.1 Network Segmentation 9
1.2 Network Device Configuration 10
1.3 Firewall Management 10
1.4 Network Device Administration 11
1.5 Wireless Networks 11
2. System Security 11
2.1 System Management 11
2.2 Secure Configuration 12
2.3 Restricted Services 12
2.4 System Vulnerability Management 13
2.4.1 Security Patch Management 13
2.5 Protection from Malicious Software 13
2.6 Mobile Computing 14
2.7 Internet of Things (IoT) 14
3. Data Security 14
3.1 Data Classification 14
3.2 Data Retention 15
3.3 Data Loss Prevention 15
3.4 Data Sharing 15
3.5 Data Encryption 16
3.5.1 Data Encryption Standards 17
3.6 Secure Data Transfer 18
3.7 Digital Certificates 18
4. Access Control, Identity and Access Management 18
4.1 Access Management 18
4.1.1 Accounts 19

4.1.2 Account Auditing 19
4.2 Password Requirements 19
4.3 Authentication 20
4.3.1 User Authentication 21
4.3.2 Administrator Authentication 21
4.3.3 Service Account Authentication 21
4.3.4 External Access Authentication 22
4.4 Remote Access 22
4.5 Physical Security 22
5. Application Development 23
5.1 Application Security 23
5.2 Secure Coding 23
5.3 Application Maintenance 24
5.4 Vulnerability Prevention 24
5.5 Application Service Providers and Vendors 25
5.6 Database Security 25
5.7 Web Services Management 25
6. Security Monitoring and Testing 25
6.1 Security Logs 26
6.2 Log Collectors 26
6.3 Security Monitoring 26
6.4 Intrusion Detection and Prevention 26
6.5 Security Audits 27
7. Operations Management 27
7.1 Change Management 27
7.2 Media Handling and Disposal 27
7.3 Data and Program Backup 28
7.4 Vendor Management 28
7.5 Personnel Security 28
8. Incident Management 29
8.1 Incident Response 29
8.2 Incident Response Plan 29
9. Security and Risk Management 29

9.1 Standards Document 29
9.2 Security Risk Assessments 29
9.3 Education and Awareness 30
9.4 Compliance 30
9.5 Security Assessments 30
9.6 Security Program Maintenance 31
EXCEPTIONS 31
DEFINITIONS 31
REVISION HISTORY 34
CONTACT INFORMATION 35
APPROVING AUTHORITY 35
REFERENCES 35

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