



BTS-2.18 - Information Classification & Protection

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

Search Code, Charter, Policy

Policy category: [Information Security](#)

Policy number: BTS-2.18

Keywords

Search

INFORMATION CLASSIFICATION & PROTECTION

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority

ARB-BTS-2.18

HISTORY

New Rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.

Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.


This rule was reviewed as part of a periodic review and remains unchanged. July 13, 2017.

This rule was reviewed as part of a periodic review and remains unchanged. August 20, 2018.

Revised by Chief Technology Officer October 10, 2018.

This rule was reviewed as part of a periodic review. September 1, 2021.

Related documents

 [BTS-2.18 Information Classification & Protection Administrative Rule](#) 120.53 KB

BTS-2.18 - Information Classification & Protection

INFORMATION CLASSIFICATION & PROTECTION

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority

ARB-BTS-2.18

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.

City Information is divided into three categories:

1. Unrestricted- (Public) Information approved for public access. This would include 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.
2. 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.

3. 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

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

Protection Measures	Information Type		
	Unrestricted (Public)	Restricted	Confidential
Access Controls	Limited to System Administration	Mandatory	Mandatory
System Maintenance	Mandatory	Mandatory	Mandatory
Logging	Mandatory	Mandatory	Mandatory
Anti-Virus	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
Labeling	Recommended	Mandatory	Mandatory

The following are necessary information security controls and processes that complement BTS Administrative Rules and standards for the protection of City information. This list is not comprehensive. Please consult with your BTS liaison or the Information Security team to ensure appropriate information security controls are applied.

Access Controls- The Bureau of Technology Services (BTS) must implement access control mechanisms for technology systems to validate appropriate authorization and authentication.

Please see BTS Administrative Rule 2.03- Network Access, BTS-2.04 - Remote Network Access, 2.05- Authorized User & Administrative Passwords and 2.06- Database Passwords for further detail.

Anti-Malware – Technology systems and services that maintain any form of City information must have anti-malware software installed, active and current. For further detail, please see BTS Administrative Rule 2.07- Malware Prevention & Recovery.

Authentication- BTS employs authentication as a key cybersecurity measure for all technology systems or services to uniquely authenticate Authorized Users. Authentication is the assurance that a party to some computerized transaction is not an impostor. Authentication typically involves using a password, certificate, Personal Identification Number (PIN), or other information that can be used to validate the identity over a technology network. Please see BTS Administrative Rule 2.05- User & Administrative Passwords for further detail on password policies.

Encryption- BTS employs encryption technologies to prevent unauthorized individuals or systems from reading or altering City information stored on City technology resources, internet-based hosted services or transmitted across City and public networks. For further guidance on appropriate encryption technologies, please see BTS Administrative Rule 2.15- Encryption and the most recent version of National Institute of Technology (NIST) Special Publication 800-57.

Firewalls- To limit intrusions and threats to the integrity and confidentiality of City information, BTS employs firewalls to secure internet and external information interfacing connections. For further detail, please see BTS Administrative Rule 2.16- Firewall Security & Management.

Labeling- Data Custodians and employees processing City Restricted or Confidential Information and media must label information according to their information classification. Failure to label documents according to their data classification may result in such documents being treated as public documents and being handled accordingly. All electronic media must be labeled prior to

storage or transmission outside the City's controlled environment. File folders containing information of various levels of classification must be labeled as the most sensitive information contained within the file folder.

All unlabeled documents will be treated as public documents and may be handled accordingly.

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.

Logging- BTS will provide appropriate collection of log information as necessary to ensure that an accurate forensic account exists regarding technology system and service activity. This logging information includes but is not limited to:

1. Changes in Authorized User groups or accounts
2. Changes to key application system files
3. Failed password attempts
4. All activity associated with Data Custodians and system administrators

Additionally, logs must be regularly reviewed by City Authorized Users responsible for maintaining these systems and services.

Physical Security- Physical security is a shared responsibility between BTS, Facilities personnel, and City employees. Physical security controls include, but is not limited to:

1. Restriction of physical access to technology systems, devices, and services, as well as paper and electronic media
2. Quarterly inventory of physical media containing Confidential and Restricted Information
3. Physical transport of media accomplished through secure courier or delivery mechanism that can be accurately tracked
4. Shredding of obsolete physical media such as paper documents and decommissioned USB devices
5. Disposal of obsolete information in accordance with the Business System Owner's information retention policy and BTS Administrative Rule 1.06- Disposal of Information Technology Equipment
6. Management and Data Custodian approval is required to move all media from a secured area.

Remote Authentication – BTS employs technology systems that support remote (off-City network) access to City information systems and resources. All remote, or telework, access must have MFA for each Authorized User account. See BTS-2.03 - Network Access and BTS AR 2.04 Remote Network Access.

System Maintenance- BTS will provide basic maintenance for technology systems and services to include, but is not limited to:

1. Changing default passwords
2. Applying software and system patches in a timely manner
3. Utilizing only necessary services on a technology system or service that stores and or transfers electronic information

References

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

- 1) BTS Technology Definitions –
<https://www.portlandoregon.gov/citycode/article/114449>
- 2) (BTS) Technology Standards Directory (and Acronyms) --
<https://www.portlandoregon.gov/bts/article/44978>
- 3) [City of Portland Information Security Standards](#)

History

New rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.

Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.

This rule was reviewed as part of a periodic review and remains unchanged. July 13, 2017.

This rule was reviewed as part of a periodic review and remains unchanged.

August 20, 2018. Reviewed and revised by Chief Information Security Officer of Bureau of Technology Services on October 23, 2018.

This rule was reviewed and revised as part of a periodic review. September 2, 2019.

This rule was reviewed and revised as part of a periodic review. June 30, 2020.

This rule was reviewed as part of a periodic review. September 1, 2021.