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 sensitive information may introduce fraud, identity theft, or other risks to the City. Since the City's sensitive 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 sensitive 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, or destruction of such information. The degree of protection provided shall correlate directly with the risk of exposure, regardless of information media type.

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

Information is divided into three categories:

1. Public- Information approved for general public access. This would include general 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 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 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.

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

	Information Type		
Protection Measures	**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	Yes (Strong authentication is preferred)
Physical Security	Recommended	Mandatory	Mandatory
Labeling	Recommended	Mandatory	Mandatory

Access Controls- Technology systems shall have mechanisms for appropriate authorization of access to information by individual users.

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

System Maintenance- Basic maintenance of electronic systems includes but is not limited to:

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

Logging- Appropriate collection of logging information is necessary to ensure that an accurate forensic account exists regarding system activity. This logging information includes but is not limited to:

- Changes in user groups or accounts
- Changes to key application system files
- Failed password attempts
- All activity associated with system administrators

Additionally, logs shall be regularly reviewed by City personnel responsible for maintaining these systems.

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

Firewalls- In order to limit intrusions and threats to the integrity of any information, firewalls shall be used to secure internet connections. For further detail, please see BTS Administrative Rule 2.16- Firewall Security & Management.

Encryption- Encryption technologies are used to prevent unauthorized individuals from reading or altering confidential or sensitive information stored on City technology resources 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.

Authentication- A key security measure for any electronic system is the means to authenticate system users. Authentication is the assurance that a party to some computerized transaction is not an impostor. Authentication typically involves using a password, certificate, PIN, or other information that can be used to validate the identity over a computer network. Please see BTS Administrative Rule 2.05- User & Administrative Passwords for further detail on password policies.

Physical Security- Includes but is not limited to:

- Restriction of physical access to paper and electronic media
- Quarterly inventory of physical media
- Physical transport of media accomplished through secure courier or delivery mechanism that can be accurately tracked
- Shredding of obsolete physical media such as paper documents
- 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
- Management approval is required to move any and all media from a secured area.

Labeling- Documents and media shall be labeled according to their data classification. All electronic media must be labeled prior to storage or transmission outside the organization. File folders containing information of various levels of classification shall have the information classified as the most sensitive information contained in the file folder.

All unlabeled documents should 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.

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.