BTS-2.18 - Data Classification & Protection

DATA 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 could 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 data 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 data.

Administrative Rule

Consistent with the 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 inappropriate 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.

Data Classification
Business System Owners are responsible for the classification of data into one of three categories. These categories allow Users, Business System Owners, Data Custodians and System Operators to understand the appropriate data handling requirements.

Data are 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 data.

2. Restricted- Information that is business data 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 data associated with internal email systems, City user account activity information and certain personnel information.

3. Confidential- Information that is very sensitive in nature and requires significant controls and protection. Unauthorized disclosure of this data 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.

Data Protection
Data are afforded different protections based on their classification. The chart below summarizes these differences:

	Data Type		
Protection Measures	**Public**	**Restricted**	**Confidential**
Access Controls	Limited to System Administration	Yes	Yes
System Maintenance	Yes	Yes	Yes
Logging	Yes	Yes	Yes
Anti-Virus	Yes	Yes	Yes
Firewalls	Yes	Yes	Yes
Encryption (during Transmission)	No	Recommended	Yes
Encryption (Storage)	No	Recommended	Yes

Authentication	Limited to System Administration	Yes	Yes (Strong authentication is preferred)
Physical Security	Recommended	Yes	Yes
Labeling	Recommended	Yes	Yes

Note: All categories marked with a "Yes" in the chart above shall mean that the associated protections are mandatory.

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

Please see BTS Administrative Rule 2.03- Network Access, 2.05- User and 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 data

Logging- Appropriate collection of logging data is necessary to ensure that an accurate forensic account exists regarding system activity. This logging data 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 data shall have anti-malware software installed, active and current. For further detail, please see BTS Administrative Rule 2.07- Malware Prevention and Recovery.

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

Encryption- Encryption technologies are used to prevent unauthorized individuals from reading or altering confidential or sensitive data stored on City systems 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 and 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 data in accordance with the Data Owner's data retention policy and BTS Administrative Rule 1.06- Disposal of Information Technology Equipment.

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 data 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 data. 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.