BTS-2.01 - Security Administrative Rule

SECURITY ADMINISTRATIVE RULE
Administrative Rule Adopted by Council
ARC-BTS-2.01

Purpose

The purpose of these Information Security Policies is to ensure the security and availability of information technology systems and networks. It also helps ensure confidentiality, integrity and availability of electronic information captured, maintained and used by the City of Portland . This policy shall be used as a foundation document for all policies, standards, procedures, and guidelines that are developed and implemented by the City, related to information security.

The Information Security Policies are to be "living" documents that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives and perceived dangers.

All users (employees, contractors, vendors, and other parties) are expected to understand and abide by these policies.

Authority and Compliance

The Chief Technology Officer (CTO) shall establish and provide authority and governance for information security policies, standards, and best practices for the City technology infrastructure in order to secure all City information systems and assets and promote the most efficient use of technology resources.

The Information Security Manager (ISM) is responsible for developing policies and standards for the implementation and use of information and telecommunications technology security standards and compliance on a Citywide basis.

The City of Portland is a public entity. It has custodial responsibilities for a significant and diverse amount of sensitive information. It holds business contracts with a broad range of public and private organizations. It is the recipient of federal and private grants. It owns, maintains and operates significant critical infrastructures and services including those of public health and safety. All of these facts place significant burden on the City regarding the management and use of its extensive information systems resources. Not least among these burdens are compliance requirements with many State and Federal laws, regulations, and promulgated rules. Pursuant to Federal and State regulations, management control of access to law enforcement data, specifically NCIC 2000 and LEDS, is under the authority of the Chief of Police of the Portland Police Bureau.

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

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

Successful compliance and protection of information systems assets requires all business system owners, system operators, data custodians and users of City owned computing, communications and network services, to learn, understand, and support this City’s information security policy and associated guidelines.

Administrative Rule

The Information Security Administrative Rules 2.02 through 2.15 include polices covering the following areas:

2.02: ROLES AND RESPONSIBILITIES
2.03: NETWORK ACCESS
2.04: REMOTE NETWORK ACCESS
2.05: USER & ADMINISTRATIVE PASSWORDS
2.06: DATABASE PASSWORDS
2.07: VIRUS PREVENTION & RECOVERY
2.08: INCIDENT REPORTING & RESPONSE
2.09: PORTABLE COMPUTING DEVICES
2.10: WIRELESS 802.11 NETWORKS
2.11: ANALOG MODEMS
2.12: PHYSICAL SECURITY
2.13: INTRUSION DETECTION
2.14: SECURITY AUDITS
2.15: ENCRYPTION

In addition to the above policies, the following general information security policies apply to all users (employees, contractors, vendors, and other parties) of the City’s information systems:

Personnel Accountability: Personnel are accountable for their actions in use of City information technologies and may be held liable to administrative or criminal sanctions for any unauthorized actions found to be intentional, malicious or grossly negligent.

Altering Authorized Access: Personnel are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges and assigned responsibilities.

Unauthorized Access: Personnel are not to access or attempt to access systems or information for which they are not authorized, nor provide access to unauthorized users. Personnel are not to attempt to receive unintended messages or access information by unauthorized means, such as impersonating another system, user or person, misuse of legal user credentials (user ids, passwords, etc.) or by causing any network component to function incorrectly. Personnel are not to possess, intercept or transfer information or communications for which they are not authorized or for which is not an assigned function of their responsibility.

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

Reconstruction of Information or Software: Personnel are not allowed to reconstruct or duplicate information or software for which they are not authorized.

Malicious Software: Personnel must not willingly or through an act of gross negligence, introduce or use malicious software such as computer viruses, trojan horses, malware or worms.

Tampering with Information Security Software and Settings: Personnel must not tamper with or disable information security software or settings, including but not limited to network password mechanisms, system logs, virus protection software, security auditing and asset management tools, system clocks, screen saver password settings and software distributions tools.

Denial of Service Actions: Personnel are not allowed to prevent authorized users or other systems from performing authorized functions by actions that deny access or the ability to communicate. These include actions that deliberately suppress communications or generate frivolous or unauthorized network traffic.

Software Licenses: All software used on City computers must be appropriately and legally acquired and used according to the licensing agreement. Possession or use of illegal copies of software or data is expressly prohibited.

Protection of Data: Personnel are required to protect the confidentiality, integrity and availability of private or sensitive electronic data they use, transmit and store. Examples of confidential, private or sensitive electronic data include but are not limited to; criminal justice data, pending litigation, employee personnel records health benefits data and medical files, credit card numbers, in-process procurement evaluation and contract negotiation materials, drivers license numbers, social security numbers, dates of birth, intellectual property and all other data expressly exempt from Oregon public records laws provided by ORS 192.501 to 192.505.

Background Checks: Background checks may be a requirement for any employee, volunteer, contractor or vendor who will be working with or around confidential or sensitive IT or communications equipment or data under BTS management. Such determination will be at the discretion of the CTO or delegate in consultation with the ISM, OM and Business System Owner unless it is mandated by law or State/Federal requirement.

Applicability

This Policy is applicable to all Business System Owners, System Operators, Data Custodians, and Users of City computing systems, networks, associated information or any other electronic processing or communications related resources or services.

Exceptions

Exceptions to this policy must be approved by the CTO or delegate in consultation with the ISM and other appropriate BTS management staff. In each case, the bureau must request the exception waiver, in writing, and include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the approval from the bureau director requesting the exception.

Monitoring of User Accounts, Files and Access

Related Administrative Rules governing employee use of information technologies and expectation of privacy, monitoring of use, site blocking, prohibited use, E-mail (including all-employee broadcast E-mail, Union use of E-mail, Netiquette, and Email records retention), and virus protection are included in the Bureau of Human Resources Administrative Rules.

Electronic Data and Records Management

Vast amounts of electronic data are in use and stored in many different forms, on computing systems and diverse data storage media. Elements of this data comprise records that are official City records. ***Records Retention and Disposition Schedules*** are promulgated by the City Auditor’s Office and can be located at http://www.portlandonline.com/auditor/

All City Business System Owners, Data Custodians, and Users are obligated to understand the nature of the data they generate, use, or store and ensure that they are managing that data in full compliance with City records management policies.

History

Authorized Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.