BTS-2.02 - Roles & Responsibilities

ROLES & RESPONSIBILITIES
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.02

Purpose

Responsibility for protecting City technology systems and data is shared by many entities and individuals throughout the City including Business System Owners, System Operators, Data Custodians, Users and the Information Security Manager.

The purpose of this policy is to describe the specific roles and responsibilities of each of these groups and individuals with regards to Information Security.

Role & Responsibilities

Information Security Manager
The Information Security Manager provides a key role of centralized oversight and enforcement for technology systems' security-related services for the City. These responsibilities include, but are not limited to the following key areas:

• Security policy development, implementation, and enforcement; including granting exceptions to any BTS Security Administrative Rule.
• Strategic security planning and plan implementation.
• Security awareness and education programs.
• Incident response services as needed.
• Security consulting services as needed.
• Development and implementation of all appropriate security standards and guidelines as necessary for the City.

Users
All Users have a critical role in the effort to protect and maintain City technology systems and data. Users of City technology resources and data have the following responsibilities:

• Support compliance with all federal and state statutes and regulations.
• Comply with all City and Bureau policies and guidelines.
• Protect all City technology assets and never share access accounts, privileges and associated passwords.
• Maintain the confidentiality of sensitive information to which they access privileges.
• Accept accountability for all activities associated with the use of their user accounts and related access privileges.
• Ensure that use of City computers, email, internet access, computer accounts, networks, and information stored, or used on any of these systems is restricted to authorized purposes and defined acceptable use policies.
• Report all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, BTS Helpdesk, Information Security Manager).
• Follow all specific policies, guidelines and procedures established by individual City bureaus and offices as well as agencies with which they are associated and that have provided them access privileges.

Business System Owners
Business System Owners play a critical role in the protection of City information systems and data. Business System Owners have responsibility for their owned systems and shall:

• Ensure compliance with all City and Bureau policies, standards and guidelines as well as all statutory and regulatory requirements.
• Define the criticality of assets and the level of security required for protection. This is determined by performing a business impact analysis of the critical functions as determined within the asset criticality guidelines
• Assign and provide necessary support and authority to appropriate staff to carry out the functions of Data Custodian(s) for all systems owned. Work in cooperation with other Business System Owners for shared systems to ensure that Data Custodian responsibilities are properly fulfilled.
• Ensure the confidentiality of sensitive proprietary data especially personally identifiable information, protected criminal justice information, and sensitive information related to protection of critical infrastructure.
• Ensure that access granted to users is based on the "Principle of Least Privilege" and "Principle of Separation of Duties" where required.
• Ensure that all incidents of security breaches are documented and reported to BTS and security services personnel.
• Document and submit any desired exceptions to citywide policy for review to the CTO.
• Support all incident response activities that involve their system(s).
• Advocate for security resources as required in City budget processes and in grant proposals.
• Define the business parameters for disaster recovery plans, including both the required recovery time and the required recovery point.
• Ensure all new employees and those granted access to City technology systems read, understand and abide by all City

policies, standards and guidelines
• Provide timely notification to BTS, System Operators and Data Custodians in events where access to City technology systems is no longer required. Such events include employment termination or job duty change.

Data Custodians
The role of Data Custodians is to provide direct authority and control over the management and use of specific information or data. The Data Custodian may be a Supervisor, Manager, or designated professional staff, assigned the responsibility by the Business Owner (Bureau Director). They may serve dual roles as a System Owner/Operator as well as a Data Custodian; however, this practice should be limited consistent with the principle of separation of duties, such that they typically would not be the technicians (system administrators) that support the related technology systems or applications. Their responsibilities include:

• Ensure compliance with all citywide and Bureau policies and all statutory and regulatory requirements.
• Provide the requirements for all access control measures related to the data they are charged with protecting to the System Operators.
• Support access control to data by acting as a single control point for all access authorization. Maintain data access authorization documentation. This document should be reviewed with the System Operator.
• Support regular review and control procedures to ensure that all users and associated access privileges are current, accurate and appropriate.
• Ensure that access granted to users is based on the "Principle of Least Privilege" and "Principle of Separation of Duties" where required.
• Ensure that data backup and retention requirements are aligned with business needs and public records rules maintained by the Auditors Office (http://www.portlandonline.com/auditor/).
• Notifies the appropriate system operators when access granted to users is no longer required.
• Data Custodians must work in conjunction with System Operators and Information Security staff to ensure that "due care" is taken to properly protect sensitive data.

System Operators
The role of System Operators is to provide day-to-day operation of a technology system. System operators, or sometimes referred to as system administrators, have the following responsibilities:

• Works with the customer (business system owner and data custodian) to understand specific security requirements as they relate to business criticality
• Works with customer (Business System Owner and Data Custodian) to identify appropriate user access to the system and data
• Works with Information Security personnel to effectively implement technologies and configurations which comply with information security policies, standards, guidelines and procedures.
• Establishes, prior to implementation, appropriate account access, technical support access, as well as backup and emergency support.
• Ensures, as appropriate, that physical and logical access security is always controlled and that robust backup and recovery mechanisms are employed.
• Regularly monitors for unauthorized access as well as maintains a history file for auditing purposes and reports any unauthorized or suspicious activity immediately to information security personnel.
• Works with the Business System Owner and Data Custodian in preparing disaster recovery plans.
• Works with the Data Custodian to define the proper data backup and retention schedule and ensures data is consistently backed up and retained in accordance with such schedules.
• Removes access to City technology systems immediately upon notification of proper events such as employee termination or reassignment of job duties.

HISTORY

Ordinance No. 179999, passed by City Council March 15, 2006 and effective April 14, 2006.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.