BTS-2.02 - Roles & Responsibilities

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

Policy category: Information Security

Policy number: BTS-2.02

ROLES & RESPONSIBILITIES

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

ARB-BTS-2.02

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.

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. April 30, 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-2.02 Roles & Responsibilities Administrative Rule 118.67 KB

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 Resources, including systems, assets, and information, is shared by many entities and individuals throughout the City including the Senior Information Security Officer, Authorized Users, Business System Owners, Data Custodians, and System Operators.

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

Role & Responsibilities

Senior Information Security Officer (SISO)
The Senior Information Security Officer 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:
1. Security policy development, implementation, and enforcement; including granting exceptions to any BTS Security Administrative Rule.
2. Strategic security planning and plan implementation.
3. Security awareness and education programs.
4. Risk assessment and incident prevention.
5. Contract review of technology acquisitions.
6. Incident response services as needed.
7. Security consulting services as needed.
8. Development and implementation of all appropriate security standards and guidelines as necessary for the City.

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

1. Support compliance with all federal and state statutes and regulations.
2. Comply with all City and Bureau rules, policies and guidelines.
3. Protect all City technology assets and information and never share access, accounts, privileges and associated passwords.
4. Always maintain the confidentiality of sensitive information for all uses.
5. See: 'List of Sensitive Information Fields' for guidance in determining confidential information. https://www.portlandoregon.gov/bts/article/731543

Accept accountability for all activities associated with the use of their Authorized User accounts and related access privileges.
6. Ensure that use of City and personal technology devices, 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.
7. Report all suspected security and/or policy violations to an appropriate authority, including your manager, the SISO r and BTS Helpdesk.
8. Follow all relevant 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.
9. Comply with all software licensing terms, rules and restrictions.

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 managed systems and internet-based services and storage and must:

1. Ensure compliance with all City and Bureau rules, policies, standards and guidelines as well as all statutory and regulatory requirements.
2. 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 and aligned to BTS Administrative Rule 2.18 INFORMATION CLASSIFICATION & PROTECTION. See: https://www.portland.gov/sites/default/files/2020-06/bts-2.18-information-classification-protection-699964.pdf
3. Assign and provide necessary support and authority to appropriate Authorized Users to carry out the functions of Data Custodian(s)* for all managed technology systems and services. Work in cooperation with other Business System Owners for shared systems to ensure that Data Custodian responsibilities are properly fulfilled.
4. Ensure the confidentiality of sensitive proprietary data especially personally identifiable information, protected criminal justice information, and sensitive information related to protection of critical infrastructure.
    a. See: ‘List of Sensitive Information Fields’ for guidance in determining confidential information. https://www.portlandoregon.gov/bts/article/731543
5. Ensure that access granted to Authorized Users is based on the “Principle of Least Privilege” and “Principle of Separation of Duties” as appropriate and where required.
6. Ensure that all incidents of security breaches are documented and reported to BTS HelpDesk and Information Security services personnel.
7. Document and submit any desired exceptions to Citywide policy for review to the CTO.
8. Support all incident response activities that involve respective managed system(s) and services.

9. Advocate for security resources as required in City budget processes and in grant proposals.
10. Define the business parameters for disaster recovery plans, including both the required recovery time objectives and the required information recovery point.
11. Ensure all new Authorized Users are provided with City policies, standards and guidelines.
12. Provide timely notification to BTS, System Operators and Data Custodians in events where access to City technology systems and services is no longer required. Such events include employment termination or job duty change.

Data Custodians (Information 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 Custodians may be a supervisor, manager, or designated professional staff, assigned the responsibility by the Business System Owners (Bureau Director). They may serve dual roles as a Business System Owners/Operators as well as a Data Custodians; however, this practice must be limited and 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, services or applications. Their responsibilities include but are not limited to:

1. Ensure compliance with all Citywide and Bureau rules, policies and all statutory and regulatory requirements.
2. Provide to System Operators and internet-based service providers the requirements for all access control measures related to the data they are charged with managing and protecting.
3. Support access control to data by acting as a single control point for all access authorization. Maintain data access authorization audit logs and documentation. These audit logs and documents must be reviewed with the System Operators or internet-based service provider.
4. Support regular review and control procedures to ensure that all Authorized Users and associated access privileges are current, accurate and appropriate.
5. Ensure that access granted to Authorized Users is based on the “Principle of Least Privilege” and “Principle of Separation of Duties” as appropriate and where required.
6. Ensure that data backup and retention requirements are aligned with business needs and public records Administrative Rules maintained by the Auditors Office (http://www.portlandonline.com/auditor/).
7. Notifies the appropriate System Operators or internet-based service provider when access granted to Authorized Users is no longer required.
8. Data Custodians must work in conjunction with System Operators, or internet-based service provider, and Information Security personnel to ensure that “due care” is taken to properly protect City Confidential Information.

System Operators, System Administrators and Internet-based Service Providers

The role of System Operators and internet-based service providers is to provide day-to-day operation of a technology system or service. System operators and internet-based service providers, also referred to as system or service administrators, have the following responsibilities:

1. Works with the bureau (Business System Owners and Data Custodians) to understand specific security requirements as they relate to business criticality, confidentiality and regulatory compliance.
2. Works with bureau (Business System Owners and Data Custodians) to identify appropriate user access to the system and data.
3. Maintains the confidentiality, integrity and availability of City Technology Resources with ongoing patching, monitoring, alerting and status reports.
4. Works with Information Security personnel to effectively implement technologies and configurations which comply with information security policies, standards, guidelines and procedures.
5. Establishes, prior to implementation, appropriate account access security, technical support access, as well as backup and emergency support.
6. Ensures, as appropriate, that physical and logical access security is always controlled, and that robust backup and recovery mechanisms are employed.
7. 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.
8. Works with the bureau (Business System Owners and Data Custodians) in preparing disaster recovery plans.
9. Works with the Data Custodians to define proper data backups and with the Auditor's office retention schedules and ensures data and information is consistently maintained in accordance with such schedules.
10. Removes access to City technology systems and Internet-based services immediately upon notification of authorized access change events such as employee termination or reassignment of job duties.

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
Authorized Ordinance No. 179999 passed by 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.
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. April 30, 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.