BTS-2.08 - Incident Reporting & Response

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

Policy category: Information Security

Policy number: BTS-2.08

INCIDENT REPORTING & RESPONSE

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

ARB-BTS-2.08

Search Code, Charter, Policy

Keywords

Search

HISTORY

Authorized by 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 Chief Technology Officer November 15, 2013.

This rule was reviewed as part of a periodic review and remains unchanged, 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. August 20, 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-2.08 Incident Reporting & Response Administrative Rule 127.16 KB

BTS-2.08 - Incident Reporting & Response

INCIDENT REPORTING & RESPONSE
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.08

Purpose
Security compromises can potentially occur at every level of computing from an individual's desktop computer or mobile device to the largest and best-protected technology systems within the City. Incidents can be accidental incursions or deliberate attempts to compromise City Technology Resources and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals, business services, systems and the City as a whole.

For the purposes of this policy an "Information Security Incident" is any accidental or malicious act with the potential to a) result in misappropriation or misuse of Confidential or personal information (compliance information, such as PCI, CJIS, FTI; attorney client privileged information, social security numbers, health records, financial transactions, etc.) b) imperil accessibility to or the functionality of City Technology Resources, c) allow unauthorized access to City resources or information, or d) allow City Technology Resources to be used to launch attacks against the resources and information of other individuals or organizations.

In the case an Information Security Incident is determined to be of potentially serious consequence, the responsibility for acting to resolve the incident and to respond to any negative impact rests with the BTS Information Security Office in cooperation with the Chief Technology Officer (CTO) rather than other specific individuals, bureaus, departments, or groups. The City has established procedures and identified the Senior Information Security Officer (SISO) as its authority in developing response plans to serious Information Security Incidents. As described below, reports of Information Security Incidents will immediately be forwarded to the SISO. The SISO follows protocols in determining what actions must be taken and depending upon the nature of the security incident will determine whether incidents should be handled within the purview of the affected bureau, Bureau of Human Resources (BHR), or by additional security and operations specialists within BTS, the Information Security Office, or through partnership with external information security incident response resources. In certain cases, the SISO may escalate the incident to the City Attorney’s Office, law enforcement, BHR, Risk Management or other City officers.

This policy outlines the procedures Authorized Users must follow to report potentially harmful Information Security Incidents. Authorized Users whose responsibilities include managing computing and communications systems have even greater responsibilities. This policy outlines their responsibilities in securing systems, monitoring and reporting Information Security Incidents, and assisting Authorized Users, Business System

Owners, Data Custodians, System Operators and Administrators, and BTS staff to resolve security incidents.

Administrative Rule
All Authorized Users must take appropriate actions to immediately report and minimize the impact of Information Security Incidents.

Reporting unlawful or improper actions of Authorized Users is expected and covered in the following Bureau of Human Resources Administrative Rules:

BHR-4.08: Information Technologies
BHR-11.01: STATEMENT OF ETHICAL CONDUCT
BHR-11.02: PROHIBITED CONDUCT
BHR-11.03: DUTY TO REPORT UNLAWFUL OR IMPROPER ACTIONS

To review the rules, access the Auditor's web site at:
http://www.portlandonline.com/auditor/index.cfm?c=26812

Responsibilities

AUTHORIZED USERS
1. Report Information Security Incidents immediately to the BTS Helpdesk. BTS support staff will help you assess the problem and determine how to proceed.
2. Do not delete anything unless told to do so.
3. Following the report, individuals must comply with directions provided by BTS support staff and/or the SISO to repair the system, restore service, and preserve evidence of the incident.
4. Individuals must not take any retaliatory action against a system or person believed to have been involved in an Information Security Incident.

BTS Support Professionals
BTS Support Professionals have additional responsibilities for Information Security Incident handling and reporting for the systems and services they manage. In the case of an Information Security Incident, BTS support staff must:

1. Respond quickly to reports from individuals.
2. Take immediate action to stop the incident from continuing or recurring.
3. Following BTS Incident Response protocols and established procedures determine whether the incident should be handled locally or reported to the SISO.
4. If the incident involves the loss of City Confidential and Restricted Information, including personal information, critical data, or has potentially serious impacts for the City, the BTS Support Professional must:

    a. Contact the Information Security Office immediately. The SISO or a delegate will investigate the incident in consultation with the CTO and relevant technology support specialists and develop an Incident Response plan.

b. File a report, using BTS' service ticketing system, including a description of the incident and documenting any actions taken. The Information Security Office may request BTS Support Professionals to complete an *Information Security Incident report form*.
c. Do not discuss the incident with others until a response plan has been formulated. The SISO and the appropriate Principle Information Officer will determine information disclosures and notices.
d. Follow the Incident Response plan to preserve evidence of the incident, repair the system(s) and restore services.

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 by 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.
This rule was reviewed as part of a periodic review and remains unchanged, 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. August 20, 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.