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 to the largest and best-protected systems in the City. Incidents can be accidental incursions or deliberate attempts to break into systems 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 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 result in misappropriation or misuse of confidential information (social security number, health records, financial transactions, etc.) of an individual or individuals, significantly imperil the functionality of the technology infrastructure of the City, provide for unauthorized access to City resources or information, 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 Chief Information Security Officer (CISO) as its authority in developing response plans to serious information security incidents. As described below, reports of information security incidents will be forwarded to the CISO. The CISO follows protocols in determining what actions should be taken and depending upon the nature of the security incident will determine whether incidents should be handled within the purview of the bureau, HR, or by additional security and operations specialists within BTS or the Information Security Office. In some cases, the CISO may escalate the incident to the City Attorney, law enforcement, human resources or other City officers.

This policy outlines the procedures individuals should follow to report potentially serious information security incidents. City employees whose responsibilities include managing computing and communications systems have even greater responsibilities. This document outlines their responsibilities in securing systems, monitoring and reporting information security incidents, and assisting individuals, administrators, and other BTS staff to resolve security problems.

Administrative Rule
All City employees shall take appropriate actions to report and minimize the impact of information security incidents.

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

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

City Employees
- Report information security incidents immediately to the BTS Helpdesk. BTS support staff will help you assess the problem and determine how to proceed.
- Following the report, individuals should comply with directions provided by BTS support staff and/or the CISO to repair the system, restore service, and preserve evidence of the incident.

- Individuals should not take any retaliatory action against a system or person believed to have been involved in an information security incident.

BTS Support Professionals

BTS technology professionals have additional responsibilities for information security incident handling and reporting for the systems they manage. In the case of an information security incident, BTS support staff should:

- Respond quickly to reports from individuals.
- Take immediate action to stop the incident from continuing or recurring.
- Determine whether the incident should be handled locally or reported to the CISO.
- If the incident involves the loss of confidential information or critical data or has other potentially serious impacts, the support specialist should:

1. Contact the Information Security Office immediately. The CISO or a delegate will investigate the incident in consultation with the CTO and relevant technology support specialists and develop a response plan.
2. File a report, using BTS' trouble ticketing system, including a description of the incident and documenting any actions taken thus far.
3. Refrain from discussing the incident with others until a response plan has been formulated.
4. Follow the response plan from the CISO to preserve evidence of the incident, repair the system(s) and restore service.

- Support staff should not take any retaliatory action against a person believed to have been involved in an information security incident.

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.