IT 17.06: Incident Response Standards

Policy Authority

BTS Administrative Rule 2.01- Security Administrative Rule
BTS Administrative Rule 2.08- Incident Reporting and Response

Purpose

Policy

Incident response process and procedures create the means for an effective response to information security incidents that affect the availability, integrity, or confidentiality of the City's information assets. This response allows the City to mitigate and/or prevent further loss or compromise of the City's information assets.

Process

In order to execute an effective information security incident response, a incident response plan that includes the following:

- Purpose
- Objectives
- Incident Categories
- Incident Response Team
  - Roles and Responsibilities
  - Activation
- Plan Creation and Review

Purpose

The purpose of an incident response plan is to identify and manage the necessary resources to deal with an adverse information security event.

Objectives

The objectives of an incident response plan are to:

- Prepare personnel for their role during an incident
- Limit and/or eliminate the impact of a given incident
- Recover from the incident
- Communicate with affected business system owners
- Reassess the incident response plan on a regular basis to ensure effectiveness

Incident Categories

An incident is categorized into one of three severity levels:

- **Level 1 (Low) -** Low level security incidents have a minimal impact to information systems or data.

The following are examples of Low level security incidents:

- Email spam- Any category of spam that can not be contained by the anti-spam server and requires additional policy guidance to contain.
- Isolated virus infections- An isolated infection is any infection that a) affects 5 or fewer workstations or servers and/or b) can be readily contained by the City's current anti-virus infrastructure.

- Vulnerabilities that can be mitigated by changes in configuration, policy, or procedure. These are vulnerabilities *not* related to systems with payment card (credit or debit card) or personally identifiable information (For example: names in combination with social security numbers).

Any Level 1 event, such as an isolated virus infection, on any system that holds cardholder or personally identifiable information, is automatically classified as a Level 3 event.

- **Level 2 (Medium)** – Medium level security incidents affect the availability of services or data.

The following are examples of Medium level security incidents:

- Widespread virus infections
- Discovered vulnerabilities, but not breaches, in systems that house:
  - Payment cardholder (debit or credit card) data
  - Personally identifiable information (For example: names in combination with social security numbers)

Any Level 2 event that involved payment card data, requires that the City follow the incident response procedures from the payment brands. These procedures are found here:

- http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html
- http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

- **Level 3 (High)** – High level security incidents affect critical information systems or data.

The following are examples of High level security incidents:

- Compromise or loss of cardholder (debit or credit card) data
- Compromise or loss of personally identifiable information (For example: names in combination social security numbers)

Incident Response Team

The incident response team provides an orderly response to incidents. Its mission is to prevent or limit losses of public confidence or information assets by providing an immediate response to security incidents.

The BTS incident response team will, at a minimum, consist of:

- Information Security Manager (ISM)
- Customer Relations Manager (CRM)
- Other BTS Personnel, such as Information Security personnel, as deemed needed by the Information Security Manager
- Business System Owner

In the case of a Level 3 incident, the City Attorney's office will need to be part of the incident response team in order to coordinate and inform the City's legal response to various regulatory issues that may arise from the compromise of cardholder and/or personally identifiable information.

The team is responsible for investigating intrusion attempts and other incidents as well as reporting findings to management, business system owners, and the

appropriate authorities as necessary. The Information Security Manager will coordinate these investigations.

- **Roles and Responsibilities**

- Information Security Manager- Authorized to make necessary changes to BTS systems or infrastructure to contain and/or eliminate a security incident. Establishes and implements the overall BTS information security plan. Responsible for convening the Incident Response Team when an incident occurs.
- Customer Relations Manager- Responsible for coordinating and issuing communications to City users and business system owners.
- City Attorney- Responsible for advising ISM and CRM on relevant privacy legislation and provides input on security incident communications to City and/or external parties
- Business System Owner- Creates initial information classification, performs periodic reclassification, and ensures regular reviews for value and updates to manage changes to risk. The business system owner is typically a non-BTS Bureau representative.

- **Activation**

The incident response team is activated for Level 2 and Level 3 events, but not for Level 1 events.

Level 1 events are handled by the functional manager who notices such limited events. However, functional managers should still report the nature and resolution of Level 1 incidents to the ISM.

The following communications should take place for the following incident categories:

Level 1- Functional owner of impacted system should communicate to the ISM the following:

- Nature and Chronology of the incident
- Affected systems
- Resolution of the incident

Level 2- Functional owner of impacted system should communicate to the CRM the following:

- Nature and Chronology of the incident
- Affected systems
- Resolution of the incident

In a Level 2 incident, the Information Security Manager is the functional owner.

Level 3- Functional owner of impacted system should communicate to a) the CRM, b) Deputy Chief Technology Officer and c) Chief Technology Officer, d) City Attorney the following:

- Nature and Chronology of the incident
- Affected systems
- Resolution of the incident

In a Level 3 incident, the Information Security Manager is the functional owner.

A Level 3 incident is likely to require legal action and/or financial restitution. Therefore, it is important to have legal counsel involved as soon as possible to assist with this part of the incident response.

Plan Creation and Review

The ISM creates and set standards related to incident response plan. In order to ensure the continued effectives and adequacy of the plan, the ISM conducts an annual review of the policy and plan. This review will also take place if significant changes occur between annual reviews. The ISM will also plan and conduct an annual exercise of the incident response plan.

Other City Bureaus may use this plan as a model for their own incident response plan.

Procedures

There are five stages to an incident response plan. These stages are described below to provide a context for understanding the lifecyle of an incident as well as how the Incident Response Team and any functional owner should track and report on any incident. These stages should be incorporated into any incident response reporting by the Incident Response Team and/or functional owner.

These stages are:

- Detection- The identification of whether an incident has occurred or not. The identification of an incident allows the functional owner and/or the Incident Response Team to decide on appropriate next steps to contain, eradicate, and recover from an incident.
- Containment- The steps necessary to limit the scope and magnitude of an incident. This should occur as soon as an incident is recognized.
- Eradication- Removal of the cause of the incident. This can involve removing a virus or a person from physical premises.
- Recovery- Restoring a system to its normal business status. Part of any recovery effort should be the successful testing of this system to verify that it has been returned to its normal condition.
- Follow-up- Communication and or operational changes necessary to ensure that all parties are informed of the lifecycle of the incident and that operating procedures are changed to ensure that such an incident does not occur again. For any incidents related to cardholder data, the ISM must notify the City's acquirer: Wells Fargo. The City's primary contact is:

Kelly Reiter
Relationship Manager
Kelly.m.reiter@wellsfargo.com
Tel: (360) 993-3759

Any loss or compromise of cardholder and/or personally identifiable information may also require further follow-up as mandated by the Oregon Identity Theft Protection Act. Information on these requirements can be found at:

http://dfcs.oregon.gov/id_theft.html

Revision History

Version	Effective Date	Authored By	Approved By	Date
1.0	7/1/09	Logan Kleier, Information Security Manager	Bureau Leadership Team	6/25/09
1.1	2/11/13	Logan Kleier, Information Security Manager	Logan Kleier, Information Security Manager	2/11/13