# Section 1: Purpose

This policy is intended to ensure that the City is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective. A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. This policy covers all incidents that may affect the security and integrity of the City's information assets, and outlines steps to take in the event of such an incident.

# Section 2: Scope

The scope of this policy covers all information assets owned or provided by the City, whether they reside on the City network or elsewhere.

# Section 3: Policy

## 1. Types of Incidents

A security incident, as it relates to the City's information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

- Electronic: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.

- Physical: A physical Information Technology (IT) security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain City information.

## 2. Preparation

Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.

Additionally, prior to an incident, the City must ensure that the following is clear to IT personnel:

- What actions to take when an incident is suspected.

- Who is responsible for responding to an incident.

The City should strongly consider having discussions with an IT Security Consultant that offers incident-response services before such an incident occurs in order to prepare an emergency service contract. This will ensure that high-end resources are quickly available during an incident.

Finally, the City should review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of customer data), and ensure that its incident response plans adhere to these regulations.

## 3. Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.

## 4. Electronic Incidents

When an electronic incident is suspected, the City's goal is to recover as quickly as possible, limit the damage done, and secure the network. The following steps should be taken in order:

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.

2. Disable the compromised account(s) as appropriate.

3. Report the incident to the IT Manager.

4. Backup all data and logs on the machine, or copy/image the machine to another system.

5. Determine exactly what happened and the scope of the incident. Was it an accident? An attack? A Virus? Was confidential data involved? Was it limited to only the system in question or was it more widespread?

6. Notify City management/executives as appropriate.

7. Contact an IT Security consultant as needed.

8. Determine how the attacker gained access and disable this access.

9. Rebuild the system, including a complete operating system reinstall.

10. Restore any needed data from the last known good backup and put the system back

online.

11. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.

12. Reflect on the incident. What can be learned? How did the Incident Response team perform? Was the policy adequate? What could be done differently?

13. Consider a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

## 5. Physical Incidents

Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable polices, such as those covering encryption and confidential data, should be reviewed.

Physical security incidents are most likely the result of a random theft of inadvertent loss by a user, but they must be treated as if they were targeted at the City.

The City must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

### a. Response

Establish the severity of the incident by determining the data stored on the missing device. This can often be done by referring to a recent backup of the device. Two important questions must be answered:

1. Was confidential data involved?
    a. If not, refer to "Loss Contained" below.
    b. If confidential data was involved, refer to "Data Loss Suspected" below.

2. Was strong encryption used?
    a. If strong encryption was used, refer to "Loss Contained" below.
    b. If not, refer to "Data Loss Suspected" below.

### b. Loss Contained

First, change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the IT Manager. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

### c. Data Loss Suspected

First, notify the executive team and legal counsel so that each team can evaluate

and prepare a response in their area.

Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred, and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

6. **Notification**
   If an electronic or physical security incident is suspected to have resulted in the loss of third-party or customer data, follow applicable regulations and/or industry breach disclosure laws.

7. **Applicability of Other Policies**
   This document is part of the City's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as needed.

## Section 4: Enforcement

This policy will be enforced by the IT Manager and/or executive team. Where crimes are suspected, the appropriate authorities will be notified. Violations may result in disciplinary action, which may include suspension, restriction of access, or more-severe penalties up to and including termination of employment.

## Section 5: Definitions

**Encryption:** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

**Malware:** Short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.

**Mobile Device:** A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

**PDA:** Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar and notes.

**Smartphone:** A mobile telephone that offers additional applications, such as PDA functions and email.

**Trojan:** Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbors a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

**Virus:** Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

**WEP:** Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

**WPA:** Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.