# **Data Security Breach Incident Management Plan**

# **SECTION 1: GOVERNANCE**

## **OVERVIEW:**

## This document outlines the procedures and responses for real and suspected data security breaches.

## **WHEN TO USE THIS DOCUMENT:**

## This plan is intended to be scalable. Its use is not necessary for every security incident, as many incidents are small and routine, requiring only the attention of the community and information services director. It is left to the judgment of the city manager, or designee, to determine when to activate the procedures in this plan.

## **DEFINITION OF ROLES:**

* **City Manager** – Responsible for the oversight of the incident investigation. The city manager may delegate this role.
* **Law Director** – May provide legal guidance to the city manager and staff investigators.
* **Community and Information Services Director -** Responsible for the hands-on incident response and reports to the city manager.
* **Police Chief –** Assist with, or appoint an officer to assist in the investigation.
* **External Entities** – Sometimes, external entities are required to aid in the response for a significant incident. These entities will be contacted on a per-incident basis, and will be involved as deemed appropriate. Examples of external entities are, but not limited to: Sycamore Community Schools, Internet Service Providers (ISPs), Security Solutions Vendors, law enforcement (e.g. FBI and DHS), and Miami Valley Risk Management Association (MVRMA).

## **CHARACTERISTICS OF “SIGNIFICANT” OR “HIGH-VISIBILITY” INCIDENTS:**

This plan will almost always be activated for all “significant” or “high-visibility” incidents. This is an inherently subjective criterion, so individual judgment is required. However, for the purposes of guidance, some examples of such incidents include, but are not limited to:

* Incidents involving key City officials and staff such as City Council members, department heads, or other staff serving in highly visible positions.
* Incidents for which a press release may or will be issued, or media coverage is anticipated.
* Incidents likely to result in litigation or regulatory investigation.
* Incidents involving criminal activity.
* Any other incident that is likely to involve reputational, regulatory, and/or financial risk to the City of Montgomery of which senior management should be aware.

## **EMPLOYEE RESPONSIBILITIES:**

Every City staff member has the responsibility to immediately report suspected or known information security incidents, or breaches of the privacy or security of restricted information to their department head and the community and information services director. Criminal acts, such as thefts, or suspected criminal acts, should also be reported to the police department.

## **RESPONSIBILITIES FOR INCIDENT RESPONSE**

1. Upon initial determination of a possible security incident, staff shall notify the community and information services director and the city manager immediately.
2. The city manager is responsible for the execution of all the sections of this plan that are applicable to the specific incident, and may deviate from this plan, after consultation with the community and information services director, police department, law director, or external entities to the extent necessary to respond to the incident.
3. As one of their first actions, the city manager shall consult with legal counsel to identify possible conflicts of interest in the investigation. Counsel should also be consulted regarding possible law enforcement involvement, and/or the need for forensic investigation.
4. The city manager or designee shall consult with MVRMA to determine if they should be engaged in the response.
5. The city manager or designee shall ensure that resources are assigned to conduct the investigation, as applicable to the incident. In the event of possible conflicts of interest, those resources must be sufficiently independent to avoid the appearance of a conflict of interest.
6. For electronic incidents, the community and information services director, police chief, or external entities may conduct the forensic investigation.
7. The city manager or designee is responsible to ensure that, if necessary, evidence is preserved, and each incident is adequately documented.

# **SECTION 2: TRIAGE AND SCOPING**

## **OVERVIEW:**

The triage and scoping phase involves the process of analyzing the information about the situation to determine if a security incident has occurred. This section includes guidance for incident identification, initial reporting, priority-setting based on data and system criticality and severity, required collection and analysis of incident information, information preservation, documentation, and communication.

## **WHAT IS A SECURITY INCIDENT?**

A security incident may involve, but is not limited to, any or all of the following:

* + A violation of City policies and standards
  + Unauthorized system or information access
  + Loss of information confidentiality
  + Compromise of system or information integrity
  + A denial of service condition against data, network or computer
  + Misuse of service, systems or information
  + Physical or logical damage to systems, or device theft
  + Presence of an unauthorized application, such as malware
  + Unauthorized or suspicious network activity

## **INCIDENT REPORTING:**

Most incidents will not be directly reported to the city manager, but most likely will be processed through the community and information services director. If the community and information services director determines that an incident should be elevated to the city manager, the information identified in Figure 1, or as much of the information as is available, must be collected, documented, and shared.

The initial severity level may be escalated or de-escalated by the city manager. All incident reports are to be made as soon as possible after the incident is identified, and with minimum delay for medium to high severity incidents.

## **INITIAL INCIDENT REPORTS:**

Initial incident reports must include the following information when describing the incident:

* + Date and time of incident discovery
  + General description of the incident
  + Systems and/or data at possible risk
  + Actions that have been taken since incident discovery
  + Contact information
  + Any additional relevant information known at the time

Figure 1  
Incident Reporting Elements

|  |  |
| --- | --- |
| **Information to Record** | **Description** |
| Suggested Severity Level | Low, Medium, High, Critical |
| Type of Incident | Note all types that apply, including but not limited to:   1. Compromised System 2. Compromised User Credentials 3. Network Attacks (DOS, Scanning, Sniffing) 4. Malware (Viruses, Worms, Trojans) 5. Lost Equipment/Theft 6. Physical Break-in 7. Social Engineering (Phishing) 8. Law Enforcement Request 9. Policy Violation 10. Data Breach (physical or electronic) 11. Unauthorized export of controlled data |
| Incident Timeline | Date/time that the incident was discovered  Date/time that the incident was reported  Date/time or data range that the incident occurred (if known) |
| Who or what reported the event | Person or Persons: Full name and department  Automated System: Name of software package, name of the host where the software is installed, physical location of the host, system owner or department, network address of the host, and MAC address of the host if possible. |
| Incident Contact Information | List contact information for all parties involved in the incident. |
| Detailed description of the event | Include as much information as possible such as:   * Description of the incident (how it was detected, what occurred) * Description of the affected resources * Estimated technical impact of the incident (i.e. data deleted, system crashed, application unavailable) * Summary of response actions performed * Cause of the incident if known (misconfigured app, unpatched host, etc.) * List of evidence gathered * Additional non-labor costs involved in handling (estimate) * Other organizations contacted |
| Identification of the host(s) | Source of the Incident: List of source’s Host name/IP Address  Target of the Attack: Host Name/IP Address |
| Incident Handling Action Log | Include: actions taken, when, by whom |

## 

## **INCIDENT CLASSIFICATION:**

The incident classification table, Figure 2, provides several incident factors to assist in proper incident classification. Depending on the nature of the incident, some of the incident criteria represented in the table may not be present in an incident. Moreover, if an incident contains characteristics in several different severity columns, the severity of an incident must reflect the highest category.

Incident classification is a dynamic process. Incident severity may change one or more times as incident details emerge over time during the investigation process.

Figure 2  
Incident Classification Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Factors** | **Incident Severity Characteristics** | | |
| **Low** | **Medium** | **High** |
| Criticality – Application | Internal Systems and Applications | Internal or External Systems and Applications | Internal or External Systems and Applications |
| Criticality – Infrastructure | User system | Non-critical enterprise system | Critical enterprise system |
| Criticality – Infrastructure | No | Limited Scope | City-wide impact |
| Impact – User/System | Affects few people or few systems | Department-wide impact | City-wide impact |
| Impact – Public | None | Potential Impact | Definite Impact |
| Countermeasures | Solutions are readily available | Weak countermeasures | No countermeasures |
| Resolution Procedures | Available and well-defined | Resolution procedure not well-defined, bypass available | No resolution procedures or bypass available |
| Information Sensitivity | Affects an individual employee or unit | Affects an individual department | City-wide, Statewide or National impact |
| Protected Information (Personally- Identifiable Information or Protected Health Information) | None | Possible | Definite |

## 

## **CONTAINMENT STRATEGY:**

A containment strategy must be implemented that will limit the damage to City resources. The containment strategy must include contact information for various personnel who may be involved in incident response. Containment may involve a combination of technical controls, such as network and system disconnects, as well as media and communications to the public and to staff, depending upon the scope of the breach.

## 

## **PRESERVATION OF EVIDENCE:**

Consideration should be given to preserving evidence during the Triage and Scoping Phase, particularly if it becomes apparent that the incident involves criminal activity. Containment, however, takes precedence over preservation while the incident is active. Proper preservation of evidence requires establishment of chain of custody procedures prior to an incident. Any electronic evidence should be properly tracked in a documented and repeatable process.

## **INCIDENT DOCUMENTATION:**

The importance of adequate and sufficiently-detailed documentation cannot be over-emphasized, especially if regulatory investigation(s) or lawsuit(s) arise because of the incident. Consideration must be given to dedicating a single, full-time resource to adequately document the decisions that are made, and the actions taken, particularly for larger incidents.

## **IDENTIFY AND ENGAGE RELEVANT EXPERTISE:**

Identifying and engaging groups and individuals with relevant expertise is critical to accurately triage an incident and determine its scope. In large or complex cases, the City should consider bringing in a third party, such as an external organization to assist in the triage and scoping effort. To comply with terms of liability insurance, MVRMA may participate in the incident response activities.

## **COMMUNICATION/DISCLOSURE STRATEGY:**

Proper handling of internal and external communications is critical in the initial phases of incident response. It is quite possible that an initially small incident could grow into a large multi-site incident. It is also quite possible that a suspected incident could be determined to be unfounded.

Improper handling of communications could lead to embarrassment to the City in the event of a false positive, or could tip off any malicious attackers to cover their tracks, thus exposing the City to more risk.

Communication of incidents should be handled on a need-to-know basis, especially early on. All communications about the incident external to the City should be properly documented by the community and information services department.

Legal counsel should be consulted to determine whether the investigation will proceed under the direction of counsel and attorney-client privilege. If so, counsel will establish procedures for communication and documentation.

# 

# **SECTION 3: EXECUTION**

## **CONTAINMENT:**

The community and information services director must communicate with departments for incident containment. The city manager, community and information services director and affected department head must assess whether to disrupt services to internal or external customers.

## **FORENSIC ANALYSIS:**

Forensic analysis entails a technical examination of evidence, preservation of that evidence, preservation of the chain-of-custody of the evidence, documentation of observations, and analysis drawn from logical conclusions based on the evidence, absent opinion or conjecture. When conducting a forensic analysis, the analyst must adhere to the following principles:

* + Analysis must be an unbiased examination of the evidence submitted.
  + Chain of custody and evidence integrity is maintained thought the whole process of investigation.
  + Forensic analysis does not pronounce or imply guilt. The purpose is to determine whether indicators exist that can tie the suspect hardware or identity to the incident under investigation.
  + Report only verifiable information.
  + Be precise. Statements such as “numerous”, “many”, “multiple hundreds”, etc. should be avoided. Specifically state the finding, as well as the precise locations of information.
  + Identify the evidence being analyzed as thoroughly as possible.

# **SECTION 4: REMEDIATION AND POST-INCIDENT REVIEW**

## **RESPONSIBILITIES:**

The community and information services director will:

* + Communicate the need for remediation to responsible departments.
  + Document and review findings from incident investigation, containment and resolution activities.
  + Analyze conditions in the IT environment local to the incident, including technical, policy, and organizational aspects.
  + Prepare an action plan for recommended changes to improve the organization environment going forward.
  + Document lessons learned, including aspects that were good as well as those which were problematic.

## 

## **TECHNICAL ACTIONS:**

Specific technical review activities should include:

* Review whether remediation of affected local system(s) is complete.
  + Vulnerable hardware or software has been hardened against any break-ins, future attacks, or other security issues (e.g. installed patches, updated versions, replaced vulnerable sections of code).
* Conduct a root-cause analysis.
* Assess whether security vulnerabilities can be adequately remediated by making changes within the current environment or a new/replacement environment should be created.
* Take needed actions to restore essential systems to functioning status, either in the original or a repaired environment, or determine that the activities must cease or be suspended until a different or rebuilt environment can be created.
* Identify any areas where different technical measures would have prevented the breach or improved results in this environment. Also identify what technical measures worked well.
* Share lessons learned with appropriate contacts.

# 

# **APPENDIX A:**

# **DEFINITIONS:**

# Denial of Service (DoS) - is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one–and often thousands of-unique IP addresses.

# Enterprise system - The overall combination of computer hardware and software that the City uses to organize and run its operations. Enterprise systems provide core services used across the organization and on which other applications or business processes often are dependent.

# Malware - software that is intended to damage or disable computers and computer systems.

# Phishing - A form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, or other communication channels.

# Social Engineering - is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.