If you have questions or comments, please contact:

Tony Campbell
Enterprise IT Security Specialist
tcampbell@rochestermn.gov
(507) 328-2848

Section 8: INCIDENT MANAGEMENT

Section 8: Incident Management

It is critical that the City has the capability to respond quickly, minimize harm, comply with breach-related state laws and federal regulations, and maintain defined procedures in the face of an information security-related incident. The purpose of this section is to define incident management requirements.

Goals of Section 8: Incident Management

- Define information security incident.
- Ensure that information security incidents receive appropriate response, and management.
- Vest authority in those charged with responding to and/or managing an information security incident.
- Ensure compliance with all applicable laws, regulations, and contractual obligations, and provide timely communications with customers, and internal support for the process.

Incident Management Policy Index

8.1. Incident Definition

8.2. Information Security Incident Classification

8.3. Information Security Incident Response Program

8.4. Incident Response Authority

8.5. Evidence Handling and Usage

8.6. Data Breach Reporting and Notification

8.0 Incident Management Policy

8.1. Incident Definition

8.1.1. An information security incident is a systems or data event that has the potential for harm to the City, our clients, our business partners, and/or the public-at-large.

8.1.2. An information security incident includes one or more of the following:

8.1.2.1. Actual or suspected unauthorized access to, unauthorized acquisition of, or unauthorized modification of data or systems.

8.1.2.2. Actual or suspected activity by an authorized or unauthorized source to systems or data that violates legal or statutory requirements.

8.2. Information Security Incident Classification

8.2.1. The basis for incident classification is by the severity relative to the impact it has on the City. If there is debate as to which level is appropriate, the City will err on the side of caution and assign the higher severity level.

8.2.2. ""Level 1"" incidents are those that could cause significant harm to the City, or the public and/or are in violation of applicable laws, regulations, or contractual obligations or involve high risk data.

8.2.2.1. ""Level 1"" incidents require immediate response once reported.

8.2.2.2. Informing the City Administrator, the Technology Steering Committee, legal counsel, and the Enterprise IT Security Specialist immediately of a "Level 1" incident is required.

8.2.2.3. If the incident involves Criminal Justice Information (CJI), the Local Agency Security Officer (LASO) must report the incident within 24 hours per the Criminal Justice Information Systems Security Policy (CSP) section 5.3 and MN BCA policy 5050.

8.2.3. "Level 2" incidents involve the compromise of, or unauthorized access to, non-critical systems or medium risk information; detection of precursor to a focused attack; believed threat of an imminent attack, or any act that is a potential violation of law, regulation, or contractual obligation.

8.2.3.1. "Level 2" incidents require a response within 48 hours.

8.2.3.2. Informing the Technology Steering Committee, legal counsel and the Enterprise IT Security Specialist of Level Two incidents is required.

Information Security Incident Response Program

8.3.1. An organization Incident Response Plan (IRP) will ensure that information security incidents receive due response and management.

8.3.2. The Enterprise IT Security Specialist is responsible for the establishment and maintenance of an IRP.

8.3.3. The IRP will include instructions, procedures, and guidance related to preparation, identification, containment, eradication, recovery, and lessons learned.

8.3.4. All employees, contractors, consultants, and vendors should receive incident response training appropriate to their role.

8.3.5. The IRP requires annual review by the Technology Steering Committee.

8.4. Incident Response Authority

8.4.1. The Technology Steering Committee will appoint Incident Response Team members and identify their roles.

8.4.2. All responders must participate in recurring drills and exercises annually.

8.4.3. During a security incident, as well as during drills and exercises, incident management and incident response-related duties for IR Team Members should supersede normal duties.

8.5. Evidence Handling and Usage

8.5.1. All evidence, logs, and data associated with the incident require handling as follows:

8.5.1.1. Labeling of all evidence, logs, and data associated with the incident is required.

8.5.1.2. All evidence, logs, and data associated with the incident require storage in a limited access location.

8.5.1.3. All evidence handling requires written access logs (Chain of Custody).

8.5.2. The Technology Steering Committee and legal counsel have the authority to engage outside expertise for forensic evidence handling investigation and analysis.

8.5.3. Only authorized legal counsel may grant exceptions to this policy.

8.6. Data Breach Reporting and Notification

8.6.1. It is the intent of the City to comply with all information security breach-related laws, regulations, and contractual obligations.

8.6.2. The City Administrator has the authority to engage outside expertise for legal counsel, crisis management, public relations, and communications.

8.6.4. Legal counsel, in collaboration with the City Administrator, will make the determination regarding the scope and content of customer notification.

8.6.5. Legal counsel and the human resources department will collaborate on all internal and external notifications and communications. The City Administrator will authorize these publications.

8.6.7. The City Administrator, or designee, is the official spokesperson for the organization. In his/her absence, legal counsel will function as the official spokesperson.