INCIDENT RESPONSE POLICY

City of Helena/Lewis and Clark County IT&S

IT&S Information Security Policy Manual

Version Control

Policy Code:	ITSEC007	Approved By:	IT&S Steering Committee 3/24/2021 IT Board 4/8/2021
Owner:	IT&S	Effective Date:	4/8/2021

Revision History

Date	Version	Created by	Description of change

Table of Contents

1. Purpose and Scope

The purpose of this policy is to establish roles, responsibilities, and a framework for reducing risk and negative impact associated with security incidents that affect sensitive information and City of Helena/Lewis and Clark County IT&S (IT&S) technology resources. This policy addresses cybersecurity incident preparation, identification, response, and follow-up procedures.

This document applies to all IT&S employees and technology resources such as workstations, applications, servers, databases, etc.

2. Definition of Information Security Incident

In order to clearly identify what constitutes an "Information Security Incident" in the context of this IR Plan, IT&S endorses the following definition:

An Information Security Incident is defined by a single or a series of unauthorized or unexpected information security events that have a significant probability of compromising business operations and/or threatening data security. This may include but is not limited to any unauthorized access, use, modification, or control of IT&S resources, any violation of IT&S security policies, or any attempt to defeat security mechanisms or exploit vulnerabilities which affects the confidentiality, integrity, and/or availability of IT&S resources and assets.

3. Integration with Business Continuity

This IR Plan is intended to align with IT&S Business Continuity Policy and related procedures. There could be an event that triggers the need to activate both this IR Plan as well as the *Business Continuity Policy* and related recovery plans. An example of this would be a cyber-attack that causes prolonged system outage and disrupts operations for an extended period of time. Based on the severity of the incident, the Security Incident Response Team will determine whether it is necessary to activate the *Business Continuity Policy*. Refer to the *Business Continuity Policy* for information regarding how City of Helena/Lewis and Clark County will respond and recover in the event of a disaster or other event that disrupts operations.

4. Roles and Responsibilities

IT&S will perform basic incident response procedures internally, but may contract external service providers, as necessary, to assist with handling incidents.
These services may include, but are not limited to:

- Computer forensics
- Advanced incident analysis
- Legal services
- Public relations management
- Incident containment and eradication
- Vulnerability mitigation

4.1 IT Security Committee

The IT Security Committee members include: City Manager, CAO, IT&S Director, Network Managers, Helpdesk Manager, and other Persons responsible for security aspects of the enterprise. This committee is responsible for the following:

- Preparing and maintaining policy guidelines for establishing and implementing incident response procedures.
- Overseeing and coordinating the incident management activities of the Security Incident Response Team (SIRT).
- Maintaining and escalating communication, as necessary, with top management and relevant third party authorities.
- Delegating relevant tasks pertaining to specific security incidents.
- Determining if incident follow-up is needed.
- Organizing SIRT meetings.
- Reviewing the performance of the SIRT and making suggestions for improvements.
- Producing relevant documentation of security incidents (i.e., incident reports.)
- Conduct annual meetings to review security initiatives, discuss reported security incidents or vulnerabilities, and develop action plans to meet information security goals and improve incident response plans.

4.2 Security Incident Response Team (SIRT)

The SIRT is responsible for the preparation, handling, logging, and reporting of information security incidents as per this policy.

The SIRT will be comprised of members of the IT Security Committee and additional staff members, and external third parties as necessary.

The SIRT is responsible for the following incident response activities:

- Reviewing the quality and effectiveness of incident management activities and procedures.
- Maintaining up-to-date knowledge pertaining to attack vectors, incident signs, and their sources.
- Communicating the incident response requirements outlined within this policy to IT&S employees.
- Determining the incident communication process for internal and external parties. This includes defining when, what, and to whom to communicate incident response information.
- Conduct annual meetings to review security initiatives, discuss reported security incidents or vulnerabilities, and develop action plans to meet information security goals and improve incident response plans.
- Carrying out incident response procedures in accordance with the requirements of this policy.

4.3 IT&S Department

The Security Officer is the assigned individual(s) responsible for initially responding to reported cybersecurity incidents, ensuring proper incident logging, and following up to minimize the risk of a specific type of incident reoccurring in the future. The Security Officer is responsible for the following phases of incident response:

- Initial response and analysis of reported incidents.
- Convening the SIRT.
- Containing security incidents.
- Collecting evidence.
- Eradicating the incident by identifying and mitigating vulnerabilities that were exploited, removing malware, etc.
- Facilitating the recovery from security incidents by restoring affected systems, data, business processes, etc.
- Communicating status of response and investigation activities to the IT Security Committee.
- Communicating status of response and investigation activities to the IT&S Team.
- Overseeing IR training and testing.

4.4 Users

Users are responsible for immediately reporting suspected cybersecurity incidents to the Security Officer or Helpdesk. For expediency purposes, communication is preferable by phone.

4.5 Media Response

In the case of a security incident or data breach, media outlets may contact City of Helena/Lewis and Clark County employees to discuss the incident. All media response shall be handled by the Communications and Community Outreach Coordinator/PIO only. It is the responsibility of all employees to direct media questions to the Communications and Community Outreach Coordinator/PIO.

5. Incident Response Preparation

Ensuring that all individuals involved with incident response are prepared to handle their responsibilities is critical to maintaining a well-functioning program. For this reason, training and testing will be an on-going element of incident response. IT&S employees will be trained accordingly.

5.1 Prevention

The Operations Manager will ensure that appropriate anti-virus software is implemented and kept up-to-date on workstations, servers, etc. to protect from malicious software. This includes reviewing anti-virus alerts and/or reports. Patches will be applied in a timely manner on all systems as per the *Asset Management Policy*. Vulnerability scans will be performed on all systems as per the *Information Security Policy*. Additionally, secure configurations will be used on all systems.

5.2 Training

Effective incident response hinges on the proper detection and identification of incidents. Such critical elements require the accurate distinction between normal events and security related incidents. Therefore, it is critical that all IT&S employees are trained accordingly.

The Security Operations Center will create and communicate basic incident detection and reporting training for all users. Upon the annual review of IT&S' performance surrounding incident response, any noted deficiencies will be analyzed to identify gaps in the effectiveness of IT&S' training.

IT Staff and key members of incident response plans may be provided with will be provided with regular (or periodic) specialized security training at the discretion of the IT Director or Security Officer. The Security Officer is required to have up to date knowledge pertaining to attack vectors, incident signs, including precursors and indicators, and their sources.

5.3 Testing

At least once per year, a test of IT&S' incident response capabilities will be conducted. Such training may include incident response workshops, tabletop exercises, or "Fire Drills" which allow staff to actively practice incident response procedures and receive constructive feedback. Tests will include "lessons learned" to identify gaps and areas for improvement.

The Security Officer is responsible for organizing the annual Computer Security Incident Response Test, analyzing the results, and communicating the results to the IT Director.

6. Incident Identification

The proper identification and timely reporting of security incidents is necessary to ensure immediate and effective response. This also ensures the appropriate resources are utilized to control, eliminate, and determine the root cause of events that adversely impact the availability, confidentiality, or integrity, of sensitive data and IT&S' technology resources.

6.1 Detection

Through proactive monitoring as per IT&S' *Audit Controls Policy*, the IT&S Department and Security Operations Center may note suspicious log entries, files, or other signs of unusual or suspicious activity. Cybersecurity Incidents may also be detected through the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) as well as a Security Information and Event Management (SIEM) tool.

Users may detect IT Security Incidents by observing unusual or suspicious activity relating to workstations, mobile devices, applications, secure areas, etc.

6.2 Reporting

Users are required to immediately report all suspected or confirmed IT Security Incidents to the IT&S Team. Users can report incidents at 447-8300 and/or helpdesk@lccountymt.gov.

The IT&S Team is responsible for gathering information from the person reporting the incident, logging the event, and assigning an initial Incident Classification and Prioritization. Subsequent information will then be shared with the Security Officer who will then notify the appropriate members of the SIRT.

7. Classification

As Information Security Incidents vary in nature and intent, it is impractical to develop step-by-step instructions for handling every possible incident. Therefore, it is useful to categorize them by common incident types.

The following categories are not all-inclusive, but provide an initial classification in which the SIRT may use to define specific handling procedures.

Type	Description
Policy Violations	▪ Violation of policies, such as the Acceptable Use Policy. ▪ Inappropriate use of corporate assets such as computers, networks, the Internet, or applications. ▪ Unauthorized escalation of privileges or a deliberate attempt to subvert access controls.
Lost/Stolen Device	▪ A lost or stolen laptop, mobile device, or other hardware asset.
Malware	▪ A virus or worm typically affecting multiple corporate devices.
Email Abuse	▪ Spoofed email, SPAM, phishing email, and other email security-related events.
Denial of Service	▪ DOS or DDOS attack.
Compromised Information/Asset	▪ Attempted or successful destruction, corruption, or disclosure of sensitive information. ▪ Compromised host (root account, Trojan, rootkit), network device, application, or user account.
Unlawful Activity	▪ Theft / Fraud / Human Safety ▪ Cybersecurity Incidents of a potentially criminal nature, which may require involving law enforcement.
Unauthorized Access	▪ Logical or physical access without permission to a network, system, application, data, or other resource

When a Cybersecurity Incident falls into multiple categories, the category that appears to be most relevant, or the element of the incident that may have the greatest impact, should be used.

8. Incident Prioritization

Prioritization of cybersecurity incidents is one of the most critical decision points in the incident handling process. Using the system's criticality within IT&S' List of Critical Systems and considering the sensitivity of information related to the system, the SIRT will prioritize the incident based upon the potential impact and urgency.

8.1 Severity Table

Information Security Incidents are prioritized utilizing the following five-tiered severity scale:

Priority	Severity Level	Response Time	Resolution Time
P1	Critical	Immediate	8 Hours
P2	High	20 Minutes	24 Hours
P3	Medium	2 Hours	3 Days
P4	Low	4 Hours	1 Week
P5	Informational	1 day	1 Month

8.2 Impact/Urgency Matrix

The following priority matrix may be used to determine the severity level of incidents:

		Impact		
		High	Moderate	Low
Urgency	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P5

(P1 = Priority Level 1)

8.2.1 Impact

Impact addresses the potential effect an incident is likely to have on staff, customers, reputation of the City/County government, or financial position. In the event that an incident falls under multiple scenarios, the most severe scenario will be chosen.

Impact	Description
High	▪ A system classified as having a "High" criticality is affected ▪ Confidential, restricted, or any regulated (e.g., ePHI, PCI, PII) information may be exfiltrated ▪ A significant number (≥ 50%) of staff or customers are affected ▪ Damage to reputation or goodwill of the City/County government is expected to be high ▪ Financial impact of the incident is likely to be $10,000
Moderate	▪ A system classified as having a "Medium" criticality is affected ▪ Potential disclosure of internal use information ▪ A moderate number of staff or customers are affected ▪ There is moderate damage to City/County government reputation or goodwill expected ▪ Financial impact of the incident is likely to exceed $1,000, but less than $5,000
Low	▪ A system classified as having a "Low" or "Minimal" criticality is affected ▪ Only information classified as public may be exfiltrated ▪ A minimal number (≤ 10%) of staff or customers are affected ▪ There is minimal to zero impact to the City/County government's reputation or goodwill ▪ The financial impact is expected to be less than $1,000

8.2.2 Urgency

Urgency is the measure of time it takes a cybersecurity incident to have an impact on business.

Urgency	Description
High	▪ The damage caused by the incident increases rapidly ▪ Work that cannot be completed is highly time sensitive ▪ Immediate action can prevent a lower impact incident from becoming a high impact incident
Medium	▪ The damage caused by the incident increases considerably over time ▪ The work that cannot be done is moderately time sensitive
Low	▪ The damage caused by the incident only marginally increases over time ▪ Work that cannot be completed is not time sensitive

9. Response Procedures

The nature of a cybersecurity incident could vary greatly, so it is impossible to formulate a step-by-step procedure for every possible type of incident. However, the SIRT may use this common procedure as a framework to form a response to an incident. These steps, however, may be iterative as findings lead to collection of new information, and evaluations lead to new courses of actions to contain or remediate.

1. Assess and determine whether an incident has occurred
    a. Analyze the precursors and indictors
    b. Look for correlating information
2. Report to IT&S Team
    a. Upon initial suspicion that an incident has occurred, Users must immediately notify the IT&S Team
3. Classify and prioritize
    a. The IT&S Team will classify and prioritize the incident
    b. Create an event log item for the incident
4. Report to the Security Officer:
    a. Incidents will be reported to the Security Officer and IT Director
    b. Based on the severity of the incident, the Security Officer and IT Director will determine whether the incident should be escalated to the IT Steering Committee which will convene and notify other relevant internal and external stakeholders as needed.
5. Contain the incident
    a. Limit and prevent further damage by restricting access and isolating the problematic area, device, network, suspected individual, etc. from non-affected systems.
    b. Stop all functionality and capabilities of infected systems
    c. Containment may include physical isolation (e.g., controlling physical access to resources, removal of an Ethernet cable or phone line) or logical isolation, through the use of firewalls, routers, and other technology controls.
6. Collect evidence
    a. Acquire, preserve, secure, and document any evidence relating to the incident.
    b. Perform system backup and take forensic images of affected systems. This may require outsourcing forensics services. The SIRT will determine whether external forensics support is necessary.
    c. The SIRT should follow the evidence preservation guidelines included in the Appendix of this document to ensure evidence is properly preserved.
    d. Evidence preservation is not limited to a specific IR phase and may also occur throughout other response phases and activities.
7. Eradicate the incident
    a. Identify and mitigate all vulnerabilities or other weaknesses that were exploited or determined to the root cause of the incident to prevent reoccurrence.
    b. Methods for eradicating incidents may include:
        - Adding/removing firewall rules.
        - Reviewing and correcting system configurations.
        - Scanning systems to identify and remove malware.
        - Scanning systems for vulnerabilities and applying system/software updates.
        - Resetting passwords for compromised accounts.
    c. If more affected hosts are discovered (e.g. new malware infections), repeat steps 1.a and 1.b to identify all other affected hosts, then contain and eradicate the incident for them
8. Recover from the incident
    a. Return affected systems to an operationally ready state

   b. Recovery may involve rebuilding systems and restoring backups, removing any temporary firewall rules applied during containment, reconnecting systems to the network, implementing additional monitoring tools, etc.
   c. Confirm that the affected systems are functioning normally
   d. If necessary, implement additional tools to detect and deter future related activity
9. Create a follow-up report
   a. Document each phase of the incident response process. Who, what, when, where, why, and how?
10. Hold a lessons-learned meeting
   a. Review incident response process and relevant documentation among SIRT.
   b. Discuss response performance and make suggestions for improvement

10. Documentation and Follow-Up

The documentation and review of incident response procedures is essential to maintaining an effective security program. All cybersecurity incidents, or related incidents involving sensitive information, will be documented upon the reporting of any suspicious activity or potential incidents.

The following sections provide guidelines for documenting security incidents and subsequent meeting requirements.

10.1 Security Incident Log

The Security Officer will maintain an incident log containing all relevant information pertaining to both active and resolved incidents. The incident log should include the following:

- The current status of the incident
- A summary of the incident
- Contributing factors to the incident
- Actions taken by all incident handlers on the incident
- Impact assessments related to the incident
- Contact information for involved parties
- A list of evidence gathered
- Recommendations and next steps to be taken
- Additional comments from incident handlers

An incident log must be started once a security incident is identified, and then updated throughout response activities.

10.2 Meetings

The IT Security Committee will convene at least annually, to review recent security incidents, discuss response capabilities, and revise policies and procedures as needed.

10.3 Lessons Learned

Following the conclusion of every Critical or High priority incident, the SIRT will convene to discuss lessons learned. Incidents of lesser priority shall be discussed at quarterly SIRT meetings. The following questions may be asked during the reflection process:

1. Was the response time adequate following the initial detection?
2. Were notification processes followed? Were relevant managers and staff kept informed of the incident and response status?
3. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?

4. What input information was needed sooner?
5. Were any steps or actions taken that might have inhibited the recovery?
6. What would the staff and management do differently the next time a similar incident occurs?
7. What corrective actions can prevent similar incidents in the future?
8. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

11. Notifications and Communications

In the event of an incident, it is critical that relevant parties are notified and key stakeholders remain informed throughout the incident response lifecycle. Incident-related information is considered “need to know” and confidential. The following sections include contact details for internal and external parties that may need to be notified and updated throughout response activities.

11.1 Internal Correspondence

In the event of an incident, it is critical that relevant parties are notified within the appropriate timeframes as stated within this policy. The Security Officer or a delegate will lead internal communications, including notifying senior management, and provide ongoing status reports.

This section contains a prioritized list of internal correspondence.

11.1.1 Security Officer

The HIPAA Security Officer preferred contact method is by telephone:

[Name]
[Telephone Number]
[Email]

11.1.2 IT Security Committee Contact Information

The [JOB TITLE] preferred contact method is by telephone:

[Name]
[Telephone Number]
[Email]

11.1.3 High-Level Manager Contact Information

The [JOB TITLE] preferred contact method is by telephone:

[Name]
[Telephone Number]
[Email]

11.1.4 SIRT Contact Information

This section includes the contact information for all primary and alternate SIRT member.

Primary SIRT	Alternate
Primary: John Doe, Senior Network Analyst	Alternate: Jane Doe, Network Analyst
Role: Phone: Mobile: Email:	Role: Phone: Mobile: Email:
Name:	Alternate:

Role: Phone: Mobile: Email:	

11.2 External Correspondence

Depending on the nature of the incident, communication with other outside parties may be necessary. Upon the detection of incidents with a Critical, High, or Medium priority, the IT Manager must notify all relevant service providers and external parties, as appropriate. These include, but are not limited to:

- Law Enforcement
- Incident Reporting Organizations
- Internet Service Providers
- Software Vendors
- Affected External Parties

11.2.1 [Third Party Vendor]

[JOB TITLE] preferred contact method is by telephone:

[Name]
[Telephone Number]
[Email]
[URL]
[Office Hours]
[SLA]
[Response Request Process]

11.3 Contact with Authorities

The IT&S Director will be responsible for leading any necessary contact and communications with regulatory agencies and other legal authorities as needed. Relevant agencies include:

- Local/State/Federal Agencies

12. Policy Maintenance and Management

The owner of this document must evaluate and perform any necessary updates to this document at least once per year. The owner may delegate tasks related to this policy as appropriate.

- The Security Officer will adhere to the continual validation, review, and updating of this policy.
- When evaluating the effectiveness, the number of discrepancies involving the reporting and treatment of incidents as well as violations of the requirements outlined within this policy.
- Upon formal review of this policy, the Security Officer must perform any necessary revisions and proceed to properly communicate policy changes throughout the organization as necessary.

13. References

NIST Cybersecurity Framework References

- PR.IP – Information Protection Processes and Procedures
- DE.AE – Anomalies and Events
- DE.CM – Security Continuous Monitoring
- DE.DP – Detection Processes RS.RP – Response Planning
- RS.CO - Communications
- RS.AN – Analysis
- RS.MI – Mitigation
- RS.IM - Improvements

Policy References

- Asset Management Policy
- Information Security Policy

14. Appendix : Evidence Preservation Guidelines

To ensure digital evidence is appropriately preserved prior to the arrival of a trained forensics specialist, response personnel must act in accordance with the following guidelines:

Don't:

- ✓ **Don't turn the computer or smartphone OFF** if it's on
- ✓ **Don't turn the computer or smartphone ON** if it's off
- ✓ **Don't leave the device in an open area** or other unsecured space
- ✓ **Don't remove or plug in** memory cards, USB thumb drives, or any other storage media
- ✓ **Don't leave wireless devices or cell phones** in an area where they could get cellular or wireless signal
- ✓ **Don't click on files, view photos or open applications**
- ✓ **Don't copy files** to or from the smartphone or computer
- ✓ **Don't let anyone without forensic training investigate** or view files on the original device
- ✓ Above all, **don't wait** to preserve evidence!

Do:

- ✓ **Act quickly**; time is of the essence
- ✓ **Call a trained digital forensic specialist** right away
- ✓ **Cast a wide net.** Preserve any and all digital evidence that you think may be useful down the road. Remember, preservation is relatively inexpensive, and you can decide later whether you want to analyze it.
- ✓ **Place a Preservation Order** as soon as you think you may need data from a device, application or network that belongs to someone else

If you have access to a device containing electronic evidence that you would like to preserve:

- ✓ **Take a photograph of the evidence** (including front, back, etc.) as soon as possible so that you can document its condition
- ✓ **Physically store evidence securely** in an access-controlled location, if it is in your or your client's possession
- ✓ **Collect loose items** (hard drives, memory cards, etc.) and place them in an evidence bag. Fill out a Chain of Custody form
- ✓ **Place items that connect wirelessly** (cell phone, laptop, tablet) in a shielded evidence bag
- ✓ **Disconnect network cables** from desktop computers