Incident Response Policy

January 29, 2025

GTEL Advisors, LLC

6120 Berkshire Lane North
Plymouth, Minnesota 55446
Phone: 612-386-4141
1/29/2025

Table of Contents

1. Introduction

The [Agency name] Technical Incident Response Policy (the "Policy") provides a framework for identifying, responding to, and recovering from technical security incidents that may threaten the integrity, confidentiality, or availability of agency systems and data. This Policy ensures that the agency is prepared to handle security incidents in a manner that minimizes damage, mitigates risk, and complies with relevant regulations, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Criminal Justice Information Systems (CJIS) Security Policy.

2. Purpose of the Policy

The primary objectives of this policy are to:

- Define the processes for detecting, responding to, and recovering from security incidents affecting agency technology systems.
- Ensure that incidents are handled efficiently and in compliance with the NIST Cybersecurity Framework and the CJIS Security Policy.
- Mitigate the impact of security incidents on operations, systems, and sensitive data, including Criminal Justice Information (CJI).
- Promote continuous improvement in security incident handling through post-incident analysis and lessons learned.

3. Scope

This Policy applies to all employees, contractors, and third-party service providers who access [Agency name] technology systems. It covers all technology systems and infrastructure, including:

- Servers, workstations, and mobile devices
- Network infrastructure, including wireless and remote access
- Cloud services and third-party applications
- Any system or platform that processes, stores, or transmits agency data, including sensitive or regulated data such as CJI

This Policy applies to all security incidents that affect or have the potential to affect the confidentiality, integrity, or availability of [Agency name]'s information systems, including those involving CJI.

4. Governance and Compliance

4.1 NIST Cybersecurity Framework

[Agency name] adheres to the NIST Cybersecurity Framework (CSF) to manage and mitigate cybersecurity risks. This Policy incorporates NIST's five key functions as follows:

1. Identify: Assess and understand the risks to agency systems and data, and establish a structured incident response process.
2. Protect: Implement preventative controls to reduce the likelihood and impact of incidents.
3. Detect: Continuously monitor and detect potential incidents or anomalies in systems.
4. Respond: Respond to incidents in an efficient, effective, and coordinated manner.
5. Recover: Implement recovery procedures to restore systems and data to normal operation after an incident.

4.2 Criminal Justice Information Systems (CJIS) Compliance

As [Agency name] handles or may have access to Criminal Justice Information (CJI), compliance with the CJIS Security Policy is critical. The policy mandates strict controls on the access, transmission, and protection of CJI, including during an incident response. All incident response activities related to CJI must comply with CJIS standards, including:

- Incident detection, analysis, and containment procedures.
- Timely notification of security breaches to relevant law enforcement or regulatory bodies.
- Ensuring the confidentiality and integrity of CJI throughout the response and recovery process.

5. Incident Response Plan Overview

5.1 Definition of a Security Incident

A security incident is defined as any event that compromises or has the potential to compromise the security of [Agency name]'s systems, networks, or data. This includes but is not limited to:

- Data breaches or unauthorized access to sensitive information.
- Malware infections or ransomware attacks.
- Denial-of-service attacks.
- Physical security breaches affecting technology infrastructure.

5.2 Roles and Responsibilities

The following roles are critical in the incident response process:

- Incident Response Team (IRT): A dedicated team composed of security personnel, IT staff, legal, and management to coordinate and respond to security incidents.
- Security Analysts: Personnel responsible for identifying and analyzing incidents.
- IT Support: Personnel responsible for mitigating the impact of incidents on systems and networks.

- Legal and Compliance Officers: Responsible for ensuring that the response complies with regulatory requirements, including CJIS.

5.3 Incident Response Phases

The incident response process consists of the following phases:

1. Preparation: Establishment of incident response plans, policies, and tools.
2. Detection and Identification: Recognizing and confirming an incident.
3. Containment: Preventing further damage by isolating affected systems.
4. Eradication: Removing the root cause of the incident.
5. Recovery: Restoring affected systems and services to normal operation.
6. Post-Incident Analysis: Analyzing the incident to improve future responses.

6. Incident Detection and Reporting

6.1 Incident Detection

Incidents can be detected through:

- Automated monitoring tools for system anomalies, network traffic analysis, and alert systems.
- Manual reporting from employees or contractors observing suspicious activity or system degradation.
- Third-party notifications from vendors, partners, or government agencies.

6.2 Incident Reporting Procedure

Once an incident is detected, it must be immediately reported using the following procedure:

1. Internal Reporting: Employees must immediately notify the IT help desk or designated incident response contact (e.g., security team).
2. Incident Logging: Details of the incident should be logged, including the nature of the event, affected systems, and the time of discovery.
3. Escalation: Incidents that pose significant risk or involve sensitive data must be escalated to the Incident Response Team (IRT) for further action.

7. Incident Analysis and Mitigation

7.1 Initial Assessment and Classification

Upon receiving an incident report, the IRT should:

- Assess Severity: Classify the incident based on its severity and impact on business operations, systems, and data.
- Prioritize: Prioritize incidents according to the potential harm to sensitive data, including CJI.

7.2 Containment and Mitigation

Containment strategies may include:

- Disconnecting compromised systems from the network.
- Implementing network segmentation or firewall rules to isolate affected systems.
- Restricting user access to limit the spread of the incident.

7.3 Root Cause Analysis

Once containment is achieved, the IRT should conduct a root cause analysis to identify how the incident occurred and any vulnerabilities that were exploited.

8. Communication and Documentation

8.1 Internal Communication

During an incident, clear internal communication is essential to ensure coordinated efforts. Key communications include:

- Regular status updates to management and affected departments.
- Coordination between security, IT, and legal teams.

8.2 External Communication

External communications may include:

- Notifications to law enforcement or regulatory bodies, especially when CJI is involved.
- Public disclosure or notification to affected individuals, as required by law or regulation.

8.3 Documentation and Record-Keeping

All actions taken during the incident response must be thoroughly documented, including:

- Incident logs, analysis, and mitigation steps.
- Communication records.
- Post-incident review reports.

9. Recovery and Remediation

9.1 System Restoration

Systems should be restored based on predefined recovery plans, ensuring that the integrity of the data is maintained throughout the recovery process.

9.2 Data Recovery and Validation

Data recovery procedures should be implemented to restore any lost or compromised data. Validation checks should ensure that recovered data is accurate and complete.

9.3 Continuous Monitoring

After recovery, systems should be continuously monitored for any signs of reoccurrence or lingering threats.

10. Post-Incident Activities

10.1 Incident Review and Lessons Learned

After the incident is resolved, the IRT should conduct a thorough review to:

- Evaluate the effectiveness of the response.
- Identify weaknesses in the process or security controls.
- Implement improvements to prevent similar incidents in the future.

10.2 Reporting and Compliance

A final report should be prepared that includes an incident summary, actions taken, impact assessment, and any corrective actions. This report may be required for regulatory compliance, particularly under CJIS guidelines.

11. Training and Awareness

11.1 Ongoing Training Programs

[Agency name] will regularly conduct training on incident response procedures, tools, and awareness to ensure that all employees understand their roles during a security incident.

11.2 Employee Awareness

Employees should be educated about the signs of potential security incidents, how to report them, and the importance of timely communication during an incident.

12. Policy Violations and Enforcement

Violations of this policy, including failure to report incidents or non-compliance with response procedures, will be subject to disciplinary action. Violations may also result in legal consequences, depending on the severity of the incident.