5.3 Incident Response (IR) Policy

PURPOSE

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities. Agencies shall track, document, and report incidents to appropriate agency officials and/or authorities.

POLICY

01. INCIDENT RESPONSE TRAINING

1. Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources.
2. The [*agency name*] shall provide incident response training to system users consistent with assigned roles and responsibilities:
3. Prior to the user assuming an incident response role or responsibility.
4. Acquiring system access.
5. Annually, thereafter.
6. Training needs to be reviewed and updated annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
7. Provide incident response training on how to identify and respond to a breach, including the organization’s process for reporting a breach.

02. INCIDENT RESPONSE TESTING

1. Agencies test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on the agency’s operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes
2. The [*agency name*] shall test the effectiveness of the incident response capability for the system annually using [tabletop, walk-through exercises, simulations, or other agency-appropriate tests]. Results should be documented and reviewed.
3. Coordinate incident response testing with organizational elements responsible for related plans, i.e., business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, critical infrastructure plans, etc.

03. INCIDENT HANDLING

1. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
	1. Coordinate incident handling activities with contingency planning activities.
	2. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
	3. Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

04. INCIDENT MONITORING

1. Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.
2. Track and document incidents.

05. INCIDENT REPORTING

1. The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.
2. The [*agency name*] shall require personnel to report suspected incidents to the incident response capability immediately, but not to exceed one (1) hour after discovery.
3. Report security incident information to the [*agency name*] LASO or organizational personnel with security responsibilities, and if confirmed, notify the MSP ISO.
4. Report incidents using automated mechanisms.
5. Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

06. INCIDENT RESPONSE ASSISTANCE

1. Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services.
2. The [*agency name*] shall provide an incident response support resource, integral to the incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

07. INCIDENT RESPONSE PLAN

1. It is important that agencies develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, agencies consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain.
2. The [*agency name*] shall develop an incident response plan that:
3. Provides the [*agency name*] with a roadmap for implementing its incident response capability.
4. Describes the structure of the incident response capability.
5. Provides a high-level approach for how the incident response capability fits into the overall organization.
6. Meets the unique requirements of the agency which relate to mission, size, structure, and functions.
7. Defines reportable incidents.
8. Provides metrics for measuring the incident response capability within the agency.
9. Defines the resources and management support needed to effectively maintain and mature an incident response capability.
10. Addresses the sharing of incident information.
11. Is reviewed and approved by the agency head annually.
12. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities.
13. The [*agency name*] shall distribute copies of the incident response plan to organizational personnel with incident handling responsibilities.
14. Review the incident response plan annually.
15. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
16. Communicate incident response plan changes to organizational personnel with incident handling responsibilities (identified by name and/or by role).
17. Protect the incident response plan for unauthorized disclosure and modification.

Incident Response Plan Breaches

1. Determine if notice to individuals or other organizations is needed.
2. Assess to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals. Also, look at mechanisms to mitigate such harms.
3. Identification of applicable privacy requirements.

PROCEDURES

Agency must provide the procedures on how the policies will be implemented.

COMPLIANCE

Agencies are required to review and update the current incident response policy and procedure annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.