**Incident Response Policy and Procedures (IR)**

**IR-1: Incident Response Policy and Procedures**

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [*Assignment: organization defined frequency]:*

a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Control Translation: Ensure incident response policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the incident response policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Incident Response Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**IR-2: Incident Response Training**

NIST SP 800-53 Objective: The organization:

a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and

b. Provides refresher training [Assignment: organization-defined frequency].

Control Translation: Ensure incident response training is in place.

Notes: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.

How to test and evaluate: Examine SSP and Incident Response Policy (if available) and verify that it is documented that incident response training is in place. Verify that organization incorporates simulated events into incident response training and automated mechanism is employed to provide a thorough and realistic training environment.

Technology specific: General

**IR-3: Incident Response Testing and Exercises**

NIST SP 800-53 Objective: The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.

Control Translation: Ensure incident response tests and exercises are in place.

Notes: Related control: AT-2.

How to test and evaluate: Examine SSP and Incident Response Policy (if available) and verify that it is documented that incident response tests and exercises are in place. Verify that organization tests and/or exercises the incident response capability in accordance to the organization-defined frequency and that organization follows the organization-defined tests and/or exercises.

Technology specific: General

**IR-4: Incident Handling**

NIST SP 800-53 Objective: The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Control Translation: Ensure incident handling capability is in place and that it coordinates with contingency planning activities.

Notes: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related control: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

How to test and evaluate: Examine SSP and Incident Response Policy (if available) and verify that it is documented that incident handling capability is in place and that it coordinates with contingency planning activities. Verify that lessons learned are incorporated into incident response procedures, training, and testing/exercises.

Technology specific: General

**IR-5: Incident Monitoring**

NIST SP 800-53 Objective: The organization tracks and documents information system security incidents.

Control Translation: Ensure incident handling monitoring capability is in place and that security incidents are tracked and documented.

Notes: Documenting information system security incidents includes, for example maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related control: AU-6, AU-7, SI-4.

How to test and evaluate: Examine SSP and Incident Response Policy (if available) and verify that it is documented that incident handling monitoring capability is in place and that security incidents are tracked and documented. Verify that any deficiencies identified are added to the POA&M as needed. Note if organization has automated mechanisms employed to assist in tracking of security incidents. If not, note how security incidents are tracked and documented.

Technology specific: General

**IR-6: Incident Reporting**

NIST SP 800-53 Objective: The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and
2. Reports security incident information to designated authorities.

Control Translation: Ensure incident reporting capability is in place and that security incidents are reported to designated authorities.

Notes: The intent of this to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related control: IR-4, IR-5.

How to test and evaluate: Examine SSP and Incident Response Policy (if available) and verify that it is documented that incident reporting capability is in place and that security incidents are reported to designated authorities. Verify that suspected security incidents are reported to the response capability within the organization-defined time-period. Note if automated mechanism is employed to assist in the reporting of security incidents. If not, note the process of organization’s incident reporting capability.

Technology specific: General

**IR-7: Incident Response Assistance**

NIST SP 800-53 Objective: The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Control Translation: Ensure incident response assistance capability is in place and that security incidents are tracked and documented.

Notes: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related control: IR-4, IR-6.

How to test and evaluate: Examine SSP and Incident Response Policy (if available) and verify that it is documented that incident response assistance capability is in place and that security incidents are tracked and documented. Note if organization have automated mechanism employed that will assist in incident response assistance support. If not, note the security incident assistance capability to external providers.

Technology specific: General

**IR-8: Incident Response Plan**

NIST SP 800-53 Objective: The organization:

1. Develops an incident response plan that:
   * Provides the organization with roadmap for implementing its incident response capability;
   * Describes the structure and organization of the incident response capability;
   * Provides a high-level approach for how the incident response capability fits into the overall organization;
   * Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   * Defines reportable incidents;
   * Provides metrics for measuring the incident response capability within the organization;
   * Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   * Is reviewed and approved by designated officials within the organization;
2. Distributes copies of the incident response plan to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements];
3. Reviews the incident response plan [Assignment: organization-defined frequency];
4. d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
5. e. Communicates incident response plan changes to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements].

Control Translation: Ensure incident response plan is in place.

Notes: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization’s mission, strategies, and goals for incident response help determine the structure of its incident response capability.

How to test and evaluate: Examine SSP and Incident Response Policy (if available) and verify that incident response plan is in place. Verify that plan is reviewed and updated according to organization defined-frequency and that plan is distributed to personnel responsible for incident response capabilities.

Technology specific: General