



FedRAMP Moderate Templates

Incident Response Implementation Checklist

Policy and Documentation

- ☐ **IR-1:** Develop organization-wide incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- ☐ **IR-1:** Ensure incident response policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- ☐ **IR-1:** Document procedures to facilitate implementation of the incident response policy and associated controls
- ☐ **IR-1:** Disseminate incident response policy and procedures to organization-defined personnel or roles
- ☐ **IR-1:** Designate the ISSO or equivalent to manage the development, documentation, and dissemination of the incident response policy and procedures
- ☐ **IR-1:** Review and update incident response policy at least every 3 years or when changes occur
- ☐ **IR-1:** Review and update incident response procedures at least annually or when changes occur
- ☐ **IR-8:** Develop an incident response plan that provides the organization with a roadmap for implementing its incident response capability
- ☐ **IR-8:** Describe the structure and organization of the incident response capability in the plan
- ☐ **IR-8:** Provide a high-level approach for how the incident response capability fits into the overall organization
- ☐ **IR-8:** Ensure the incident response plan meets the unique requirements of the organization related to mission, size, structure, and functions
- ☐ **IR-8:** Define reportable incidents in the incident response plan
- ☐ **IR-8:** Provide metrics for measuring the incident response capability within the organization
- ☐ **IR-8:** Define the resources and management support needed to effectively maintain and mature an incident response capability
- ☐ **IR-8:** Address the sharing of incident information in the incident response plan



FedRAMP Moderate Templates

- ☐ **IR-8:** Have the incident response plan reviewed and approved by the ISSO or equivalent at least every 3 years or when changes occur
- ☐ **IR-8:** Explicitly designate responsibility for incident response to the ISSO or equivalent
- ☐ **IR-8:** Distribute copies of the incident response plan to the incident response team and those with incident response roles and responsibilities
- ☐ **IR-8:** Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing
- ☐ **IR-8:** Communicate incident response plan changes to the incident response team and those with incident response roles and responsibilities
- ☐ **IR-8:** Protect the incident response plan from unauthorized disclosure and modification

Training and Testing

- ☐ **IR-2:** Provide incident response training to system users consistent with assigned roles and responsibilities within 10 days of assuming an incident response role or responsibility or acquiring system access
- ☐ **IR-2:** Provide incident response training when required by system changes
- ☐ **IR-2:** Provide incident response training at least annually to personnel with incident response roles and responsibilities
- ☐ **IR-2:** Review and update incident response training content at least annually or when changes occur
- ☐ **IR-3:** Test the effectiveness of the incident response capability for the system at least annually using test scenarios based on current threat information
- ☐ **IR-3(2):** Coordinate incident response testing with organizational elements responsible for related plans

Incident Handling and Response

- ☐ **IR-4:** 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
- ☐ **IR-4:** Coordinate incident handling activities with contingency planning activities
- ☐ **IR-4:** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly



FedRAMP Moderate Templates

- ☐ **IR-4:** Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization
- ☐ **IR-4(1):** Support the incident handling process using an online incident management system
- ☐ **IR-5:** Track and document incidents
- ☐ **IR-7:** Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents
- ☐ **IR-7(1):** Increase the availability of incident response information and support using automated mechanisms for real-time support

Incident Reporting

- ☐ **IR-6:** Require personnel to report suspected incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in the US-CERT Federal Incident Notification Guidelines
- ☐ **IR-6:** Report incident information to US-CERT and other organization-defined personnel or roles
- ☐ **IR-6(1):** Report incidents using automated mechanisms supporting reporting of incidents
- ☐ **IR-6(3):** 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

Key Timeframes Summary

- ☐ **Policy review:** At least every 3 years or when changes occur
- ☐ **Procedure review:** At least annually or when changes occur
- ☐ **Training:** Within 10 days of role assumption, then at least annually
- ☐ **Testing:** At least annually
- ☐ **Incident reporting:** Per US-CERT Federal Incident Notification Guidelines