

Incident Response Plan Template

Framework for responding to cybersecurity incidents

An incident response plan provides a roadmap for implementing an effective response capability. It outlines how your organization prepares for, detects, responds to and recovers from security incidents and is required by NIST SP 800-171.

Purpose & Scope

- Describe the structure, roles and responsibilities of the incident response team.
- Define what constitutes a reportable incident and categorize severity levels.
- Explain how incident information will be shared internally and externally.
- Designate responsible parties for incident declaration, coordination and communication.
- Ensure the plan is distributed to incident response personnel and key stakeholders.
- Update the plan based on operational changes, lessons learned or regulatory updates.
- Protect the plan from unauthorized disclosure and ensure availability during an incident.

Roles & Responsibilities

- Incident Response Coordinator: leads response efforts and ensures plan execution.
- IT/Security Team: performs detection, analysis, containment, eradication and recovery tasks.
- Management/Legal: provides decision-making authority, approves public communications and engages with regulators.
- Communications Lead: manages internal and external communications, including with customers and partners.
- Third-Party Providers: assist with specialized forensics, recovery or communication tasks when necessary.

Incident Classification & Reporting

- Classify incidents based on impact and urgency (e.g., Low, Medium, High, Critical).
- Establish escalation procedures and notification timelines for each severity level.
- Document who must be notified for each category (e.g., management, customers, regulators).
- Maintain records of incident timelines, actions taken and evidence collected.

Response Procedures

- Preparation: maintain assets inventories, configure logging and define communication channels.
- Detection & Analysis: monitor alerts and logs, validate incidents and assess impact.
- Containment: isolate affected systems to prevent lateral movement and additional damage.
- Eradication: remove malicious code, close vulnerabilities and strengthen security controls.
- Recovery: restore systems from clean backups, verify integrity and resume operations.
- Post-Incident Review: capture lessons learned, update documentation and improve processes.

Training, Testing & Maintenance

- Conduct regular training and tabletop exercises to ensure teams understand roles and procedures.
- Test the plan through simulations and adjust based on gaps and observations.
- Review and update the plan annually or after significant incidents or organizational changes.