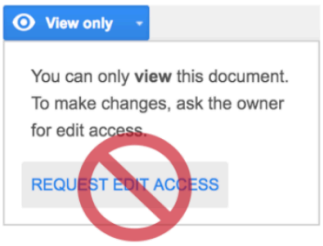
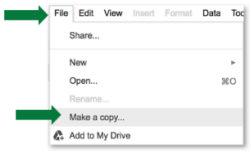
Strike Graph

Incident Response Policy Template



How to use this template:

This is a view-only file and cannot be edited. **Create your own copy** of this template to edit. In the menu, click **File > Make a copy...**



Strike Graph

Strike Graph Notes:

Our Incident Response policy template is designed to guide your organization through the essential steps of identifying, containing, investigating, and resolving security incidents. It includes detailed procedures, roles, and training requirements, along with automated tracking systems to ensure swift and effective incident management. Common pitfalls include inadequate documentation of incidents, failure to update response plans after real incidents, and unclear reporting channels.

Policy #:	Title:	Effective Date:
x.xxx	Incident Response Policy	MM/DD/YY

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. INCIDENT RESPONSE TRAINING

Strike Graph Notes:
Use this section to specify who gets IR training (e.g., SOC, IT, help desk, business incident coordinators) and realistic timelines like “within 30 days of role assignment” and “annually thereafter.” Reference your LMS, HR onboarding process, and tabletop exercises as evidence.

The [entity] shall:

a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

   i. Within [entity defined time period] of assuming an incident response role or responsibility.

   ii. When required by information system changes, and [entity defined frequency] thereafter.

b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

2. INCIDENT RESPONSE TESTING

Strike Graph Notes:
Here you define how often you run tests (e.g., annual tabletop plus periodic technical exercises) and what “entity defined tests” means in practice: tabletop scenarios, red-team exercises, DR/BCP tests, or phishing simulations. Align this with existing BCP/DR testing calendars and name the teams you coordinate with. Pitfalls include testing in silos, not documenting outcomes, or failing to track remediation of issues discovered during those exercises.

The [entity] shall:

a. Test the incident response capability for the information system [entity defined frequency] using [Assignment: entity defined tests] to determine the incident response effectiveness and documents the results.

b. Coordinate incident response testing with entity contacts responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

3. INCIDENT HANDLING

Strike Graph Notes:
This section should reference your actual incident handling playbooks and IR runbooks that follow NIST's lifecycle: prepare, detect/analyze, contain, eradicate, recover, and lesson learned. Tailor it by pointing to where those procedures live (e.g., Confluence, GRC tool) and clarifying who leads each phase. Ensure "lessons learned" feeds into updated procedures and training. A frequent pitfall is never updating playbooks after real incidents or relying on undocumented tribal knowledge.

The [entity] shall:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

b. Coordinate incident handling activities with contingency planning activities.

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

4. INCIDENT MONITORING

Strike Graph Notes:
Use this to tie your SIEM, EDR, log management tools, and ticketing system into the policy. Spell out that automated tools (e.g., SIEM rules, alert pipelines) track incidents from detection through closure, and note which team owns tuning and maintenance. Gather screenshots, logging standards, and alert routing documentation.

The [entity] shall:

a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

5. INCIDENT REPORTING

Strike Graph Notes:
Customize the reporting timeframes (e.g., “within one hour of discovery”) and define clearly who “incident response capability” and “entity defined authorities” are, internal IR team, CISO, legal, privacy officer, customers, regulators, or law enforcement. Align with contractual and regulatory notification SLAs. Gather your incident classification matrix and escalation procedures as background. Pitfalls include unrealistic reporting windows, no clear reporting channel for users, or missing legal/privacy in the escalation chain.

The [entity] shall:

a. Require personnel to report suspected security incidents to the incident response capability within [entity defined time period].

b. Report security incident information to [entity defined authorities].

6. INCIDENT RESPONSE ASSISTANCE

Strike Graph Notes:
Here you describe your central “help point” for incidents: a SOC, IR team, security mailbox, hotline, or ticket queue. Customize by naming the function, hours of coverage, and how users reach them (portal, phone, email). Link to service catalog entries and IR playbooks that describe what assistance they provide. A pitfall is naming a support resource that doesn’t actually have IR skills or capacity, or not publicizing the contact pathways internally.

The [entity] shall:

a. 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.

7. INCIDENT RESPONSE PLAN

Strike Graph Notes:
This section is about having a concrete, living incident response plan, not just this high-level policy. Use the bracketed spots to name who approves it, who receives it, and how often it’s reviewed (e.g., annually or after major incidents). Reference where the plan lives, which roles it covers, how incidents are defined and measured, and how updates are communicated. Pitfalls include outdated plans, unclear ownership, and not distributing the plan to the actual responders.

The [entity] shall:

a. Develop an incident response plan that:

   i. Provides the entity with a roadmap for implementing its incident response capability.

   ii. Describes the structure of the incident response capability.

iii. Provides a high-level approach for how the incident response capability fits into the overall entity.

iv. Meets the unique requirements of the entity, which relate to mission, size, structure, and functions.

v. Defines reportable incidents.

vi. Provides metrics for measuring the incident response capability within the entity.

vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

viii. Is reviewed and approved by [entity defined personnel or roles].

b. Distribute copies of the incident response plan to [entity defined incident response personnel (identified by name and/or by role)].

c. Review the incident response plan [entity defined frequency].

d. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.

e. Communicate incident response plan changes to [entity defined incident response personnel (identified by name and/or by role)].

f. Protect the incident response plan from unauthorized disclosure and modification.

COMPLIANCE

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.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests and confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY