# Incident Response Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The quality and integrity of [Company Name’s] incident response capabilities are used to monitor for security incidents, determine the magnitude of the threat presented by these incidents, and to respond to these incidents. Without an incident response capability, the potential exists that in the event that a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

The Incident Response Policy applies to all information systems and information system components of [Company Name]. Specifically, it includes:

* Mainframes, servers, and other devices that provide centralized computing capabilities.
* SAN, NAS, and other devices that provide centralized storage capabilities.
* Desktops, laptops, and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. A security incident response capability will be developed and implemented for all information systems that house or access [Company Name] controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:
	1. Preparation
	2. Detection
	3. Analysis
	4. Containment
	5. Eradication
	6. Recovery
	7. Post-Incident Activity
2. To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. In the event that an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations within [indicate frequency – suggest 30 days] of appointment to the team and thereafter on an [indicate frequency – suggest annually] basis.
3. Incident response will be tested [indicate frequency – suggest quarterly] through the use of tabletop exercises, [indicate frequency – suggest annually] through the use of simulation tests, and [indicate frequency – suggest every three years] through the use of a full-scale test. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.
4. Incident response plans will be reviewed and, where applicable, revised on an [indicate frequency – suggest annually] basis. Review will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

**Procedure 1**

Build an enterprise incident response team and provide training:

* + - * + Identify incident response (IR) roles.
				+ Identify incident response responsibilities.
				+ Build and deliver an incident response training program. Training should address:

How to recognize an incident.

How to analyze an incident.

How to contain and eradicate an incident.

How to return to normal operations.

How to communicate and escalate during an incident.

How to operate all IR tools and resources.

**Procedure 2**

Build an enterprise incident response capability.

* + - * + Create an incident response plan:

Detail plan detection phase to establish processes to be followed to discover and identify incidents.

Detail plan analysis phase to indicate the measures that are to be taken to determine and understand the nature of an incident.

Detail plan containment and eradication phase to indicate the measures that are to be taken to limit the spread of an incident and eliminate the effects of the incident.

Detail plan recovery and post-recovery phase to establish a structured return to normal operations.

* + - * + Acquire incident response tools and resources:

Identify and acquire monitoring resources such as intrusion detection systems, traffic sniffers, and log aggregators.

Identify and acquire analysis resources such as dedicated workstations and forensics software.

Identify and acquire response resources including communications devices and contact trees.

**Procedure 3**

Test enterprise incident response.

* + - * + Define testing methodologies and tests. Include the following capabilities:

Recognition of externally and internally sourced incidents.

Analysis to gather incident identification information.

Application of containment and eradication tasks appropriate to the type of incident.

Restoration of normal operations.

Co-ordination and communications.

* + - * + Execute tests. Tests can come in different forms:

Provide notice to test participants so that they can plan workload to ensure availability for the test.

Provide notice to business and IT operations staff in the event that the plan inadvertently impacts normal operations.

* + - * + Review test results and take corrective action.

**Procedure 4**

Operate the enterprise incident response capability.

* + - * + Detect incidents and identify threats:

Monitor systems for signs of incidents.

Categorize incidents according to established standards in order to establish appropriate subsequent processes.

* + - * + Analyze discovered threats:

Investigate discovered incident indicators to determine if a valid threat may occur, is occurring, or has occurred.

Fully document all aspects of the incident and incident response.

Prioritize response to incidents according to potential impact.

Notify appropriate individuals within the organization once the threat has been validated and prioritized.

* + - * + Contain threats to minimize impact and maintain operations:

Select a containment strategy appropriate to the incident, the impacted system, and the available resources.

Gather evidence to allow for further investigation as the incident progresses and once it is complete, as well as for potential prosecution.

Where time and resources permit, identify the attacker to help stop the incident as well as to prepare for potential prosecution.

* + - * + Eradicate contained threats and recover to normal operations:

Eradicate all non-evidentiary remnants of incident.

Recover affected systems to pre-incident status and return to normal operations.

Maintain heightened monitoring of the affected system(s) subsequent to an incident to ensure there are no lingering impacts.

* + - * + Perform post-recovery tasks:

Conduct forensic analysis and retain evidence.

Conduct post-mortem and take corrective action.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

#

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |