# Incident Response Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. SANS Incident Handler's Handbook: https://www.sans.org/white-papers/33901/
2. ISO/IEC 27035-2: <https://www.iso.org/standard/78974.html>
3. ISO/IEC 27037: https://www.iso.org/standard/44381.html
4. ISO/IEC 27050 series: https://www.iso.org/standard/78647.html
5. NIST SP 800-86: <https://csrc.nist.gov/pubs/sp/800/86/final>
6. NIST SP 800-61: https://www.nist.gov/privacy-framework/nist-sp-800-61
7. ISO/IEC 27001:2022: 7.4, A.5.19, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.8
8. NIST 800-53 rev. 5: AU-3, CP-10, CP-10(2), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-6(3), IR-7, IR-7(1), IR-8, IR-9, IR-9(2), IR-9(3), IR-9(4), SR-8
9. CIS v8: 14.6, 14.7, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9
10. PCI DSS 4.0: 12.10.1, 12.10.3, 12.10.4, 12.10.4.1, 12.10.6, 12.10.7
11. AICPA SOC 2 TSC: A1.3, CC2.2, CC2.3, CC4.2, CC7.3, CC7.4, CC7.5, P6.3, P6.6, P8.1

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this Incident Management Policy is to establish a framework for responding to information security incidents in a consistent and effective manner. This policy aims to minimize the impact of incidents on the organization’s operations, assets, and reputation by ensuring prompt identification, containment, eradication, recovery, and communication of incidents. By defining roles, responsibilities, and procedures, this policy supports the organization’s commitment to maintaining the confidentiality, integrity, and availability of its information assets and complying with applicable legal, regulatory, and contractual requirements.

## Scope

This policy applies to all employees, contractors, vendors, and third parties who interact with the organization’s information systems and data. It encompasses all types of information security incidents, including but not limited to unauthorized access, data breaches, malware infections, denial of service attacks, and any other incidents that could compromise the security of the organization’s information assets. This policy covers the entire incident management lifecycle, including incident response planning, detection, reporting, analysis, containment, eradication, recovery, communication, and post-incident review. The procedures outlined in this policy are mandatory and must be followed by all relevant personnel to ensure a coordinated and effective response to information security incidents.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], Operational owner title] |  |
| Information Systems Administrators | System Administrators  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. 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.
	2. 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

## Definitions

* 1. Incident Response Plan: A documented strategy detailing the actions to be taken before, during, and after an information security incident to mitigate potential damage and ensure recovery.
	2. Incident Response Team: A group of individuals within an organization responsible for responding to information security incidents, ensuring that they are contained, investigated, and resolved.
	3. Business Continuity Plan: A plan that outlines procedures to ensure that essential functions can continue during and after a disaster or other disruption.
	4. Recovery Point Objective (RPO): The maximum acceptable amount of data loss measured in time; defines the point in time to which data must be recovered to resume business operations.
	5. Recovery Time Objective (RTO): The maximum acceptable length of time that a system, application, or function can be down after a failure or disaster occurs before business continuity is negatively affected.
	6. Backup: The process of copying and archiving data to ensure it can be restored in the event of data loss or corruption.
	7. Incident Reporting: The process of notifying relevant parties about a suspected or actual security incident, providing sufficient details for assessment and response.
	8. Incident Escalation: A predefined process for escalating an incident to higher authority levels within the organization based on the severity and impact of the incident.
	9. Alert Management: The process of monitoring, prioritizing, and responding to security alerts generated by various monitoring systems to determine if they are indicative of an incident.
	10. Incident Notification: The process of informing external stakeholders, including regulatory bodies, affected users, and possibly the public, about a security incident and its implications.
	11. Disaster Recovery Plan: A documented plan that outlines how an organization will recover from a disaster and restore normal operations.
	12. Forensic Techniques: Methods used to collect, preserve, analyze, and present evidence in a way that is legally admissible, often used in incident investigations.
	13. Lessons Learned: Knowledge gained from the review of an incident or exercise that can be used to improve future incident response and preparedness efforts.
	14. Third-Party Incident Management: The process of managing incidents that involve external vendors or service providers, including communication, coordination, and resolution.
	15. Incident Simulation: A practice exercise designed to test the effectiveness of an incident response plan by simulating a real-life incident scenario.
	16. Material Incident: An incident that has significant impact on the organization’s operations, assets, or reputation, requiring special attention and reporting.
	17. Containment: The process of limiting the scope and impact of an incident to prevent further damage.
	18. Eradication: The process of removing the cause of the incident and eliminating the threat from the environment.
	19. Recovery: The actions taken to restore and validate system functionality and data integrity after an incident has been contained and eradicated.
	20. Post-Incident Review: An evaluation conducted after an incident has been resolved to analyze what occurred, why it happened, and how response efforts can be improved.
	21. Uninterruptible Power Supply (UPS): A device that provides emergency power to a load when the input power source fails, ensuring continuous operation during a power outage.

## Policy

#### Incident Response Planning

The [responsible party] shall:

* + 1. Develop, maintain, and annually review an Incident Response Plan that aligns with the organization’s mission, size, structure, and functions.
		2. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
		3. Distribute the incident response plan to all members of the Incident Response Team and relevant stakeholders.
		4. Ensure the Incident Response Plan is protected from unauthorized disclosure and modification

.

#### Incident Response Team

The [responsible party] shall:

* + 1. Designate specific roles and responsibilities for incident response within the Incident Response Plan.
		2. Ensure all personnel are trained in their incident response roles and responsibilities within a defined period of assuming the role, upon changes to the information security system, and annually thereafter.
		3. Assign the Incident Response Team responsibilities for responding to information spills and other incidents​​​​.
		4. Conduct annual incident response tests, including simulations and tabletop exercises, to evaluate the effectiveness of the IRP.
		5. Review and update the Incident Response Plan based on test results and lessons learned from actual incidents​​ .

#### Business Continuity and Disaster Recovery

The [responsible party] shall:

* + 1. Develop a Business Continuity Plan that identifies essential mission and business functions and associated contingency requirements.
		2. Establish alternate telecommunications services to permit the resumption of critical systems within defined Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
		3. Implement uninterruptible power supplies and automatic emergency lighting to ensure continuous operation and safe evacuation in the event of power outages.
		4. Establish a Backup Strategy for data and processes
		5. Develop and maintain a Disaster Recovery Plan that aligns with the organization’s business continuity strategy.
		6. Conduct annual tests of the Disaster Recovery Plan to ensure readiness and effectiveness.

#### Issue Reporting

The [responsible party] shall:

* + 1. Provide mechanisms for internal and external users to report suspected security incidents, such as a dedicated incident reporting email and hotline.
		2. Ensure all reports are logged with details, including the name of the reporter, contact information, the time of the report, and the nature of the incident​​.
		3. Require personnel to report suspected security incidents within a reasonable period of time
		4. Establish an incident ticketing system to categorize and track reported incidents.

#### Alert Management

The [responsible party] shall:

* + 1. Monitor system-generated indications of compromise continuously.
		2. Correlate information from various monitoring tools to prioritize events and determine if they constitute incidents.
		3. Alert the Security Incident Response Team upon detection of unauthorized access, data leakage, or other critical events.
		4. Assess the impact and severity of each incident to determine if it is material.
		5. Implement an escalation process to ensure incidents are promptly addressed based on severity​​​​.

#### Notification and Response

The [responsible party] shall:

* + 1. Notify relevant external stakeholders and affected users promptly in the event of a security incident.
		2. Coordinate communications with the legal team to ensure compliance with regulatory requirements.
		3. Develop and implement a communications plan for external notifications, including media communications if necessary​​ .
		4. Establish and maintain contacts with relevant law enforcement and regulatory authorities.
		5. Coordinate with authorities during incidents requiring external involvement, such as data breaches or cyber-attacks.

#### Incident Handling and Recovery

* 1. The [responsible party] shall:
		1. Implement an incident handling process that includes preparation, detection and analysis, containment, eradication, and recovery.
		2. Ensure the rigor and intensity of incident handling activities are consistent across the organization​​.

#### Forensics and Investigation

The [responsible party] shall:

* + 1. Use forensic techniques to collect and analyze evidence during incident investigations.
		2. Ensure all evidence is preserved and documented according to legal and organizational requirements.

#### Incorporation of Lessons Learned

The [responsible party] shall:

* + 1. Conduct post-incident reviews to capture lessons learned.
		2. Update incident response procedures, training, and plans based on the outcomes of these reviews​​.

#### Third-Party Incident Management

The [responsible party] shall:

* + 1. Ensure third-party vendors are contractually obligated to report incidents affecting the organization’s data or systems.
		2. Coordinate with third-party incident response teams during joint incidents to ensure effective resolution and communication.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. 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 [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |