# ISO 27001 Security Incident Management Plan

## Purpose

The purpose of this plan is to provide a framework for identifying, managing, and resolving security incidents effectively. It outlines procedures to mitigate risks, recover from incidents, and maintain compliance with legal, regulatory, and contractual obligations. By establishing clear processes and responsibilities, this plan enhances organizational resilience and fosters stakeholder trust by demonstrating a proactive approach to security challenges.

## Scope

This plan applies to all security incidents affecting the organization, including but not limited to:

* Cybersecurity threats such as malware, phishing, and ransomware attacks
* Data breaches involving sensitive or personal information
* Physical security breaches compromising organizational assets
* System or application failures impacting business continuity

## Policy Statement

The organization is committed to managing security incidents in accordance with ISO 27001 principles by:

* Establishing processes for the timely detection and reporting of incidents, leveraging frameworks and tools such as Security Information and Event Management (SIEM) systems and ticketing platforms.
* Assigning roles and responsibilities for incident management.
* Ensuring incidents are classified and prioritized based on severity and impact.
* Documenting and tracking incidents from detection to resolution.
* Implementing corrective and preventive actions to minimize future risks.

The plan includes the following six steps:

1. Detection and Reporting: Establish mechanisms for identifying potential incidents and reporting them promptly.
2. Classification and Prioritization: Assess and categorize incidents based on their severity, scope, and impact on organizational operations.
3. Investigation and Analysis: Conduct a detailed investigation to identify the root cause and determine appropriate mitigation measures.
4. Containment and Mitigation: Implement immediate actions to limit the scope and impact of the incident.
5. Resolution and Recovery: Restore affected systems, data, or processes to normal operations while ensuring vulnerabilities are addressed.
6. Post-Incident Review: Analyze the incident management process to identify lessons learned and opportunities for improvement.

## Roles and Responsibilities

* Incident Response Team Lead: Coordinates all incident management activities and ensures alignment with organizational policies.
* IT Operations Team: Supports technical containment, mitigation, and recovery efforts.
* Information Security Officer: Oversees compliance with ISO 27001 requirements and validates incident management practices.
* Legal Counsel: Provides guidance on regulatory reporting and legal considerations.
* Executive Leadership: Approves strategic decisions and allocates resources for effective incident management.

## Compliance and Monitoring

Compliance with this plan will be ensured through:

* Regular incident response drills to test the plan’s effectiveness.
* Implementation of key performance indicators (KPIs), such as:

- Average time to detect and respond to incidents.

- Number of incidents resolved within predefined timeframes.

- Frequency of repeated incidents.

Non-compliance will be documented, and corrective actions will be implemented to address identified gaps.

## Related Documentation

* Incident Response Plan
* Risk Management Policy
* Business Continuity Plan
* Access Control Policy

## Review and Revision

This plan will be reviewed annually or after significant incidents. The Incident Response Team Lead will initiate the review process, and updates will be communicated to stakeholders. All revisions will be documented and approved through a formal review process.

## Narrative Guidance

This plan emphasizes the importance of a structured approach to incident management, aligning with ISO 27001’s requirements for risk mitigation and continuous improvement. It provides organizations with a clear framework for managing security incidents effectively and ensuring operational resilience.

## Instructions for Use

* Replace placeholders with organization-specific details.
* Ensure alignment with related policies and standards.
* Tailor the plan to address unique risks and operational contexts.