Incident Response Policy

[1. Purpose 2](#_Toc669416626)

[2. Scope 3](#_Toc1475951576)

[3. Objectives 3](#_Toc413687796)

[4. Policy 3](#_Toc274670198)

[4.1 Incident Response Phases 3](#_Toc2055098500)

[4.2 Incident Classification 3](#_Toc1386203028)

[4.3 Incident Response Procedure 4](#_Toc1683614698)

[4.4 Communication and Reporting 4](#_Toc1466082991)

[4.5 Training and Awareness 4](#_Toc1492541523)

[4.6. Monitoring and Compliance 4](#_Toc582122183)

[5. Roles and Responsibilities 5](#_Toc1625585426)

[6. Enforcement 5](#_Toc452733492)

[7. Review and Revision 5](#_Toc1447416986)

[8. Document change control 5](#_Toc937182801)

# Purpose

The purpose of this Incident Response Policy is to establish a framework for detecting, responding to, and recovering from information security incidents. It aims to minimize the impact of incidents on the organization's operations, assets, and reputation.

# Scope

This policy applies to all employees, contractors, and third-party service providers involved in the organization’s operations. It covers all types of security incidents, including data breaches, malware infections, denial of service attacks, and unauthorized access.

# Objectives

The objectives of this policy are to:

* Ensure a prompt and effective response to security incidents.
* Minimize damage and reduce recovery time and costs.
* Protect the confidentiality, integrity, and availability of the organization's information.
* Comply with legal, regulatory, and contractual requirements for incident response.

# Policy

## 4.1 Incident Response Phases

The incident response process includes the following phases:

* Preparation: Establishing and maintaining an incident response capability.
* Detection and Analysis: Identifying and investigating potential security incidents.
* Containment, Eradication, and Recovery: Limiting the impact, removing threats, and restoring normal operations.
* Post-Incident Activity: Learning from the incident to improve response processes and security controls.

## 4.2 Incident Classification

* Incidents will be classified based on their severity and impact:
* Low: Incidents with minimal impact on operations or data.
* Medium: Incidents that affect multiple users or systems, causing some disruption.
* High: Incidents causing significant operational, financial, or reputational damage.
* Critical: Incidents with severe impacts, including regulatory violations or large-scale data breaches.

## 4.3 Incident Response Procedure

* Preparation:
  + Maintain an updated incident response plan and establish an incident response team.
  + Train employees on recognizing and reporting potential incidents.
  + Conduct regular security assessments and simulations.
* Detection and Analysis:
  + Monitor systems for signs of incidents (e.g., suspicious activity, alerts).
  + Analyze events to confirm if they constitute a security incident.
  + Log and track all incidents in the incident management system.
* Containment, Eradication, and Recovery:
  + Implement containment strategies to prevent further spread or damage.
  + Identify and eliminate the root cause of the incident.
  + Restore affected systems to normal operations.
  + Conduct a root cause analysis to determine how the incident occurred.
* Post-Incident Activity:
  + Document the incident details, including actions taken and lessons learned.
  + Review the incident response process and update policies and procedures if needed.
  + Provide a post-incident report to management.

## 4.4 Communication and Reporting

* **Internal Communication:** The Incident Response Coordinator will keep relevant stakeholders informed throughout the incident response process.
* **External Communication:** Legal and compliance teams will coordinate external communications, including reporting to regulatory authorities or affected individuals if required.
* **Incident Reporting:** All incidents must be reported immediately to the Incident Response Team via the designated reporting channel.

## 4.5 Training and Awareness

Regular incident response training will be provided to all relevant personnel to ensure readiness and capability in responding to incidents.

## 4.6. Monitoring and Compliance

* Periodic Audits: The IT department will regularly monitor compliance with this policy through periodic audits and checks.
* Disciplinary Action: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment. Contractors and third parties found in violation may have their contracts terminated.
* Training and Awareness: The IT department will provide regular training and awareness programs to ensure all employees understand the importance of this policy and their responsibilities.

# Roles and Responsibilities

* Incident Response Team (IRT): Responsible for managing the incident response process, including coordinating the investigation, containment, eradication, and recovery activities.
* Incident Response Coordinator: Leads the IRT, communicates with stakeholders, and ensures that incidents are documented and reported.
* IT Security Team: Provides technical support for detecting and analyzing security incidents, as well as implementing containment and recovery actions.
* Employees: Report suspected incidents immediately to the IRT or the designated security contact.

# Enforcement

Non-compliance with this policy may lead to disciplinary action, up to and including termination of employment. Contractors and third parties found in violation may have their contracts terminated. Additionally, repeated violations may result in loss of access to company networks and systems. The company reserves the right to take legal action against individuals or entities that violate this policy and cause harm to the company’s information assets.

# Review and Revision

This policy will be reviewed annually and updated as necessary to ensure it remains effective and aligned with ISO/IEC 27001 standards. The review process will involve key stakeholders, including the IT department, management, and employee representatives.

# Document change control

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reviewed by | Reviewed Date | Reason to review | Approved by | Approved Date | Designation of the approver |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |