<Logo>

<Organization Name>

**Incident Handling and Response Guide**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |
| **Version** | <Version> |
| **Prepared By** | <Name> |
| **Approved by** | <Name of Approval Authority/Board> |
| **Date Approved** | <Approval Date> |
| **Next Review Date** | <Review Date (typically a year from the approval date)> |
| **Document Classification** | Confidential/Public/Internal Use Only |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

**Table of Contents**

[Purpose 1](#_Toc179810960)

[Scope 1](#_Toc179810961)

[Objectives 2](#_Toc179810962)

[Roles and Responsibilities 3](#_Toc179810963)

[Incident Reporting and Classification 4](#_Toc179810964)

[Incident Management Process 5](#_Toc179810965)

[Incident Notification and Communication 6](#_Toc179810966)

[Incident Log 7](#_Toc179810967)

[Threat Scenarios 8](#_Toc179810968)

[Continuous Improvement 8](#_Toc179810969)

# Purpose

The purpose of this guide is to provide a systematic approach for identifying, managing, and responding to security incidents affecting <Organization Name>. This guide ensures that all necessary steps are taken to minimize the impact of such incidents on the organization, ensuring the integrity, confidentiality, and availability of information systems.

# Scope

This guide is applicable to all employees, contractors, and stakeholders involved in managing information systems within <Organization Name>. It encompasses the entire incident management lifecycle, from detection and analysis to containment, eradication, recovery, and post-incident review. It ensures compliance with **ISO 27001:2022** and provides guidelines to respond to incidents that threaten the security of organizational assets.

# Objectives

I**ncident Identification and Management**  
Ensure that security incidents are identified promptly, accurately, and efficiently, minimizing their potential impact on <Organization Name>.

**Compliance with ISO 27001:2022**  
Ensure the organization meets the security incident management requirements outlined in ISO 27001:2022, maintaining adherence to international standards for information security.

**Minimize Damage**  
Minimize the damage caused by security incidents through swift response, containment, and recovery processes, safeguarding the confidentiality, integrity, and availability of organizational data.

**Improve Response Capabilities**  
Continuously improve the incident response process through periodic reviews and lessons learned from past incidents, ensuring the organization is better prepared for future incidents.

**Ensure Accountability**  
Define roles and responsibilities clearly, ensuring that the **Incident Response Team (IRT)**, management, and relevant stakeholders understand their duties during incident handling.

**Communication and Documentation**  
Ensure effective communication channels are in place during incidents, both internally and externally, and maintain accurate documentation for all incidents, including post-incident reviews.

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| Incident Response Team (IRT) | Leads the incident management and coordinates response activities. |
| IT Department | Provides technical support for containment, eradication, and recovery. |
| Security Operations Center (SOC) | Monitors and detects potential incidents. |
| Legal and Compliance | Ensures legal requirements are met and liaises with external parties. |
| HR Department | Manages internal communications and employee relations. |
| Top Management | Provides oversight and strategic direction during major incidents. |
| <Role> | <Responsibility> |
| <Role> | <Responsibility> |

# Incident Reporting and Classification

The incident should be classified as follows, so that appropriate response measures can be taken based on the severity of the incident and its impact on organizational operations, data integrity, and confidentiality.

|  |  |
| --- | --- |
| **Incident Reporting Mechanism** | *Email (security@example.com), internal tool, hotline* |
| **Reporting Deadline** | *Immediately, within 30 minutes of discovery* |
| **Incident Reported By** | <Title/ Department> |
| **Incident Date/Time** | <Title/ Department> |
| **Incident Description** | <DD/MM/YYYY> at <HH> |
| **Incident Classification** | Low/Medium/High |
| **Classification Criteria** | Low/Medium/High |
| *Low - Minor data loss, no critical system affected*  *Medium - Partial system failure, sensitive data involved High - Major disruption, significant data breach, critical systems impacted* |
| **Assigned Priority** | Low/Medium/High |
| **Immediate Actions Taken** | *Disconnected affected system, isolated network* |
| **Response Team Notified** | <Department> |
| **Incident Resolution Timeframe** | Low/Medium/High |
| *Low - 24 hours Medium - 8-12 hours High - 4 hours* |
| **External Notification Requirement** | Yes/No |
| **Incident Report Log ID** | < Auto-generated or manually assigned> |

**Incident Classification** is determined based on the impact on business operations, data integrity, and confidentiality. This table provides a clear breakdown of incident severity levels and the criteria for each.

**Immediate Reporting** of any incident ensures timely response and helps prevent escalation.

# Incident Management Process

When an incident occurs, relevant parties should act according with the given process with the lead of the responsible team.

|  |  |  |
| --- | --- | --- |
| **Phase** | **Actions** | **Responsible Team** |
| Identification | Identify and verify potential incidents through monitoring and reporting tools. | SOC, IT Dept. |
| Containment | Limit the spread of the incident by isolating affected systems or networks. | IRT, IT Dept. |
| Eradication | Remove the root cause of the incident (e.g., malware removal, patch vulnerabilities). | IT Dept. |
| Recovery | Restore affected systems and services to normal operation. Validate the integrity of data and systems. | IT Dept., IRT |
| Post-Incident Review | Conduct a review to identify lessons learned and update policies or procedures. | IRT, Top Management |

# Incident Notification and Communication

In case of an Incident following parties should be notified accordingly, as given in the following table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Communication Type** | **Stakeholders** | **Purpose** | **Frequency** | **Method** |
| Internal Communication | Department Heads, Management | Provide regular updates on the status of the incident and actions taken to contain and resolve it. | *Every 1-2 hours, as the situation evolves* | *Email* |
| Incident Response Team Updates | IRT Members | Continuous updates on the progress of the incident and coordination of recovery steps. |  |  |
| Board-Level Notification | Executive Management, CISO | Inform senior management about the impact and progress of major incidents. |  |  |
| External Notification (Regulatory Bodies) | Regulatory Agencies (e.g., Data Protection Authorities) | Notify regulatory authorities about data breaches or other incidents that require reporting under legal obligations. |  |  |
| External Notification (Clients) | Affected Clients, Third Parties | Inform clients about any incident that has affected their data or services. |  |  |
| Public/Media Communication | Media, Public Relations | If needed, provide statements to the media regarding the incident. |  |  |

***Note****: This communication plan can be adapted based on the organizational structure, requirements, available resources, and legal or regulatory obligations*

# Incident Log

A detailed incident log should be maintained for every security incident as follows.

|  |  |
| --- | --- |
| **Incident ID** | <Auto-generated or manually assigned> |
| **Date and Time of Detection** | <DD/MM/YYYY> at <HH:MM:SS> |
| **Affected Systems** | <List of systems> |
| **Incident Description** |  |
| **Actions Taken** |  |
| **Responsible Personnel** | <Title> |
| <Name> |
| **Incident Classification** | Low/Medium/High |
| *Classification of the incident based on severity* |
| **Final Resolution** |  |
| **Lessons Learned** |  |
| **Incident Closed Date** | <DD/MM/YYYY> |
| **Evidence/Documentation** | *Incident report document, system logs* |

**Incident ID**

Ensures each incident is uniquely tracked for reference.

**Date and Time of Detection**

Helps analyze response times and identify trends.

**Actions Taken**

Clearly document immediate containment and eradication steps.

**Lessons Learned**

Critical for improving future incident response strategies and security measures.

# Threat Scenarios

The organization may face specific threat scenarios that require special response considerations. The possible scenarios must be documented.

|  |  |
| --- | --- |
| **Scenario** | **Response Considerations** |
| *Loss of Data Communication due to IT Network Attack* | *Immediate containment to restore communication channels, followed by network security assessments and potential hardware replacements.* |
| <Scenario> |  |
| <Scenario> |  |
| <Scenario> |  |
| <Scenario> |  |

# Continuous Improvement

The **Incident Handling and Response Guide** will be reviewed and updated annually or after any major incident to ensure continuous improvement in line with ISO 27001:2022 requirements.

**Appendix 1: Post-Incident Review Template**

|  |  |
| --- | --- |
| **Incident Summary** | <Description of the incident, impact, and resolution> |
| **Response Effectiveness** | <Evaluation of how well the response procedures were followed> |
| **Improvements Needed** | <Recommendations for process improvements or technology upgrades> |
| **Action Items** | <List of tasks or actions to address identified issues> |

**Appendix 2: Contact Information for Incident Response Team**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Contact Info** |
| <Name> | IRT Lead | <Phone/Email> |
| <Name> | IT Support | <Phone/Email> |
| <Name> | Legal Counsel | <Phone/Email> |
| <Name> | <Role> | <Phone/Email> |
| <Name> | <Role> | <Phone/Email> |