**<Your Company Logo>**

**Incident Response Plan**

# ***Version Control Table***

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Reviewed |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

|  |  |
| --- | --- |
| **Date of Next Revision** | **<date>** |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status and at yearly intervals after that.

The version control table will show the published update date and provide a thumbnail of the significant change. CAUTION: the thumbnail is not intended to summarize the difference and is not a substitute for reading the full text.

# 

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_arxqdy8knprl)

[**Table of Contents 5**](#_1fob9te)

[**Purpose 6**](#_3znysh7)

[**Scope 6**](#_2et92p0)

[**Definitions 6**](#_tyjcwt)

[**Responsibilities 7**](#_3dy6vkm)

[**Security Incident Classification System 8**](#_1t3h5sf)

[**Incident Handling and Response Plan 9**](#_4d34og8)

[Detection 9](#_2s8eyo1)

[Analysis and Containment 9](#_17dp8vu)

[Eradication and Recovery 10](#_3rdcrjn)

[Post-Incident Activities/Closure 10](#_26in1rg)

[**Collection and Preservation of Evidence 11**](#_lnxbz9)

[**Incident Tracking and Reports 11**](#_35nkun2)

[Annual Report 12](#_1ksv4uv)

[Post-Incident Report 12](#_44sinio)

[**Preparation for the Incident 13**](#_2jxsxqh)

[Annual Training 13](#_z337ya)

[Communication Guidelines 13](#_3j2qqm3)

[**Disciplinary actions 13**](#_1y810tw)

[**Change, Review, and Update 13**](#_4i7ojhp)

[**Responsibility 13**](#_2xcytpi)

[**Reference 14**](#_1ci93xb)

[**Related Documents 14**](#_3whwml4)

# Purpose

The purpose of this plan is to ensure effective and consistent management of security incidents involving <Company> and its clients’ information and information technology resources.

# Scope

This plan applies to all company employees responsible for Security Incident Response.

# Definitions

* Incident: A security event that has the potential to impact the confidentiality, integrity, or availability of an organization's assets or operations.
* Incident Response (IR): The steps used to prepare for, detect, contain, and recover from an Incident, aimed to quickly minimize incident impact, contain damage, and remediate the cause to reduce the risk of future incidents.
* Incident Response Plan: A documented set of procedures to be followed in the event of a security incident.
* Incident Response Team: A team of professionals responsible for responding to security incidents.
* Incident Severity: A measure of the impact and urgency of a security incident, used to determine the appropriate response actions.
* Containment: The process of partial or complete isolation of affected systems, users, or applications to prevent further damage.
* Remediation: The process of minimizing the impact of a security incident by applying precise technical measures.
* Eradication: The process of removing malware traces and improving security posture to avoid reinfection or similar incidents.
* Recovery: The process of restoring affected systems, data, operations, and workflows to their normal working state.
* Post-Incident Review: An analysis of the effectiveness of the incident response effort, conducted after the incident has been resolved.
* Post-Incident Activities: Long-term actions to be implemented after the incident has been resolved aimed to improve overall security posture and increase incident readiness.

# Responsibilities

Incident Response Team:

* **Incident Response Officer** is the Incident Response specialist that has ultimate accountability for the actions of the IR Team and IR function. This person should be an executive-level employee.

Incident Response Officer is responsible for:

* + reporting to the CEO and is a peer of other C-level executives;
  + an annual summary of the incidents for the calendar year;
  + reviewing any recommendations in the post-incident report and determining additional follow-up actions;
  + leading incident response activities;
  + prevention and resolution of security incidents relating to personal data;
  + procedures of storage, processing, and auditing personal data.
* **Incident Response Manager** is the employee who leads the IR team’s efforts and coordinates activities between all of its respective groups. This individual reports to the Incident Response Officer.

Incident Response Manager is responsible for:

* + process-related training material preparation;
  + activating the IR team, and managing all parts of the IR process, from discovery, assessment, remediation, and resolution;
  + prevention and resolution of security incidents relating to information systems;
  + leading investigations into how breaches happen.
* **SOC Analyst** is a <Internal/External SOC Analyst> who detects suspicious activity and determines the nature of a threat and the extent of its penetration into the infrastructure. This individual reports to the Incident Response Manager.

SOC Analyst is responsible for:

* + monitoring networks and systems for security breaches or intrusions;
  + helping <Other SOC> Analysts detect incidents;
  + helping plan an organization’s information security strategy;
  + writing correlation rules for monitoring new types of malicious activities.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Company** | **City** | **Name** | **Contact** |
| Incident Response Officer | <Company> | <City, Country> | <Name> | <Email> |
| Incident Response Manager | <Company> | <City, Country> | <Name> | <Email> |
| <Internal/External SOC Analyst> | <Company> | <City, Country> | <Name> | <Email> |

# Security Incident Classification System

Security incidents will be classified according to incident categories and severity of incidents to determine the appropriate response. The Incident Response Officer will maintain a security incident classification scheme to describe security events and support incident tracking over time.

Four incident severity levels will be used to guide incident response: **critical**, **high**, **medium**, and **low**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident Severity | Response Time | Incident Characteristics | Initial Notification Requirements | Post-Incident Report Requirements |
| Critical | 30 minutes | Immediate significant threat to the organization's critical assets, operations, or reputation | 1. Immediate voice call with all affected parties  2. Immediate call notification of Company CEO | 1. Separate formal IR report document with incident timeline and investigation details  2. Formal email to affected parties and Company management that includes IR results, performed actions, list of recommendations |
| High | 1 hour | Immediate threat that puts in danger a single critical asset or disrupts business processes | 1. Voice call with all affected parties  2. Immediate chat or email notification of Company CEO | 1. Separate formal IR report document with incident timeline and investigation details  2. Formal email to affected parties and Company management that includes IR results, performed actions, list of recommendations |
| Medium | 2 hours | Threat that negatively affects non-critical systems and is not likely to have financial impact | 1. Formal email to affected parties that includes incident summary and action plan | 1. Formal email to affected parties and Company management that includes IR results, performed actions, list of recommendations |
| Low | 6 hours | Threat with minimal potential financial impact, unable to grow in size and scope | 1. Short message in chat to all affected parties with incident summary and action plan | 1. Formal email to affected parties and Company management that includes IR results, performed actions, list of recommendations |

# Incident Handling and Response Plan

## Detection

SOC team is responsible for promptly reporting suspected or known security incidents, including an observed or suspected security weakness in systems or services.

If there are suspected incidents, including breaches of personal identity information. In a hierarchical structure, individuals at <Tier X Analyst level> are required to report to <Tier X+1 Analyst level>. If necessary, <Tier X+1 Analyst level> then escalate issues or reports to <Tier X+2 Analyst level>. After that, the Incident Response Team must be gathered as quickly as possible. Communication is via phone, email, chats, or in person. Also, each employee must be notified in the general chat of the company so employees can provide relevant evidence and additional incident information for the Incident Response Team.

* Name, response time, date, host IP (other criteria depending on the incident).
* Description of the suspected security incident.
* Why did the incident escalate?

## Analysis and Containment

Once a potential security incident is reported or anomalous activity detected, the analysis must be performed to determine if it is indeed symptomatic of a security incident and to understand the nature of the incident for proper remediation.

Incident Response Team can:

* Contact other professionals if needed.
* Analyze and correlate as many indicators as possible. Such as monitoring network traffic to/from the host suspected of being compromised, network packet captures for more in-depth analysis, log file analysis, interviews with users and/or system administrators, etc.
* Determine the incident’s scope (How many systems are affected? Is it actively propagating? If so, how?).
* Protect other computers and information on the company network and Internet:
  + Block malicious IP address(es) / hosts / VLANs / subnets;
  + If it is critical, then disconnect from the entire network.
* Determine if any confidential data was or might have been affected.
* Take action to stop the potential loss of confidential data, if needed:
  + Changing file permissions to read-only on servers;
  + Disconnecting servers with backups from the network;
  + Stopping and disabling DBs;
  + Changing passwords for administrators;
  + Blocking the rights of users not involved in responding to incidents;
  + Forced shutdown of workstations using MDM and EDR;
  + Disconnection of non-critical services from the Internet;
  + Blocking remote VPN connections;
  + Monitoring disk and CPU activity and comparing it with the average;
  + If it became known about the beginning of the spread of the encryptor, the Incident Response Manager must immediately provide a centralized command to shutdown endpoints and then block the network.
* Identify the location and owner of the computer(s), so they can be engaged in containment, eradication, and recovery.
* Research about the specific malware or type of attack (also use the Internet).
* Perform additional forensics sufficient to characterize the incident.
* Inform clients about incidents if needed. (Clients, media, and official structures should be notified only with the CEO & PR team's approval).

## Eradication and Recovery

Once an incident is contained, all malware should be securely removed, systems should again be hardened and patched, and updates should be applied. Affected systems and devices should be restored and returned to the business environment.

Incident Response Team must:

* Preserve evidence if it has not already been done.
* Perform additional analysis as needed to complete the investigation.
* Remove the components of the incident impacting the affected systems, such as deleting the malicious code or disabling a compromised user account.
* Mitigate the attack vector, so a similar incident does not occur (for example, patch the vulnerability used to compromise the system, apply standard system hardening procedures, adjust firewall rulesets, etc.)
* Restore systems to normal operation using backup.
* Restore network access if the system was blocked during the containment phase.
* Return the system to normal operations.
* Answer the following questions:
  + When can systems be returned to production?
  + Have systems been patched, hardened, and tested?
  + Can the system be restored from a trusted backup?
  + How long will the affected systems be monitored, and what will you look for when monitoring?
  + What tools will ensure similar attacks will not reoccur?

## Post-Incident Activities/Closure

Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and relevant stakeholders (if needed) to discuss what you’ve learned from the data breach.

The following steps should be done:

* Determine lessons learned and make recommendations to prevent subsequent similar incidents.
* Determine ways to improve the management of security incidents and help prevent future incidents.
* Issue final reports.
* Archive evidence and documentation.
* Conduct analysis of Incident Response Process to find weaknesses and answer the following questions:
  + What problems arose during the incident response process? What mistakes were made?
  + What changes need to be made to the security?
  + What weakness did the breach exploit?
  + Whether to change the content of the Incident Response Plan?
  + Whether to conduct urgent training for Incident Response Team and SOC analysts?
  + How should employees be trained differently?
  + Whether to change or start using new incident detection tools?
  + How will you ensure a similar breach doesn’t happen again?
* Close out the incident.

# Collection and Preservation of Evidence

When collecting evidence, follow all appropriate Company policies and procedures.

Document all actions taken in the collection and preservation of the evidence.

For data stored on electronic media, make a mirror image or copy (depending on applicable requirements) of the media.

Perform all forensics work on the image or copy, not the original. Additional images or copies of the original can be made if needed.

# Incident Tracking and Reports

The Incident Response Manager will control an incident tracking system <Name of the incident tracking system> and record, including but not limited to the following information, about all reported security incidents:

1. **Date Of Report**
2. **Submitter Name**
3. **Title**
4. **Status**

{To do;

In progress;

Closed}

1. **Date Of Incident**

{Insert incident date and time}

1. **Notified Individuals**

{Insert notified Individuals names}

1. **Type Of Incident:**

{Exposure of information;

Alteration/destruction of information;

Network;

Stolen/lost computer equipment;

Other, use field below; or

Insert additional incident type information}

1. **Affected Systems (If applicable)**

{Insert names of systems affected by the incident}

1. **Affected Records (If applicable)**

{Insert names of records affected by the incident}

1. **Incident Description**

{Insert incident description}

1. **Impact**

{Insert incident impact}

1. **Action Description**

{Insert taken/planned actions with date and time}

1. **Resolution**

{Insert resolution/mitigation steps}

1. **Recommendation**

{Insert recommended actions that should be taken to ensure that the same incident does not happen again}

All security incidents or suspected incidents (i.e., reports of suspicious activity that upon investigation are determined not to be a security incident) will be recorded in the incident tracking system.

The incident tracking data is confidential and should be protected when stored or transmitted and disclosed only to authorized individuals.

## Annual Report

In <Defined Month> each year, the Incident Response Officer has to summarize the incidents for the previous calendar year and provide a report to the CEO. The security incident data may also be used for other reports as needed. This report will be marked as confidential.

## Post-Incident Report

The Incident Response Officer will review any recommendations in the report and determine additional follow-up actions.

Post-incident reports must be submitted to the Incident Response Officer and be marked as confidential.

The post-incident report should typically include:

* Description of the incident, its ID, link to the Incident record;
* History of Incident record processing, including timing and actions by responsible people;
* Impact and loss (including financial);
* If the resolution was effective;
* Conclusions and planned changes to the incident.

The post-incident report should be attached to the Incident Records.

# Preparation for the Incident

## Annual Training

Training must be conducted annually to ensure that all employees have a certain degree of awareness about cybersecurity and a basic level of training in dealing with a cyber crisis. Everyone also has to be aware of their roles and responsibilities in case of an event.

## Communication Guidelines

Communication templates and guidelines must be created to enable seamless communication during and after an event with the team and the third party that can be affected by the incident.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy will be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy will be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 Annex A.16.1.1 Responsibilities & Procedures.
* ISO 27001 Annex A.16.1.2 Reporting Information Security Events.
* ISO 27001 Annex A.16.1.3 Reporting Information Security Weaknesses.
* ISO 27001 Annex A.16.1.4 Assessment of & Decision on Information Security Events.
* ISO 27001 Annex A.16.1.5 Response to Information Security Incidents.
* ISO 27001 Annex A.16.1.6 Learning from Information Security Incidents.
* ISO 27001 Annex A.16.1.7 Collection of Evidence.

# Related Documents

* <Company> Incident Response Registry
* <Company> Incident Response Diagram EN
* <Company> Communication Templates and Guidelines
* <Company> Incident Response report template