**Incident Response Plan**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

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

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

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_qef1iqoez6az) **4**

[**Scope**](#_rbq0oisysk5v) **4**

[**Policy**](#_s0pz43qog50e) **4**

[**Incident Response Team**](#_jnmm9bsuir6e) **4**

[**Incident Response Workflow**](#_39wyiegbqtm1) **4**

[**Agenda of Response Meeting**](#_5dvx04wm4p3c) **5**

[**Change, Review, and Update**](#_w1o88vxspwq8) **6**

[**Disciplinary Action**](#_cig3lmaq4wje) **6**

[**Responsibility**](#_yzbyhmk7n9hk) **6**

[**Related documents**](#_zh49kgk2td3a) **6**

# 

# **Purpose**

This document offers guidance for employees or incident responders who believe they have discovered or responded to a security incident. The Incident Response Plan includes specific incident response, business recovery, continuity procedures, and data backup processes. The Incident Response Plan provides coverage and response mechanisms for all critical system components and all other critical IT resources.

# **Scope**

This policy applies throughout the company as part of the corporate governance framework. It is relevant to IT users and administrators and applies to all computing platforms. This policy also applies to third-party employees working for the company.

# **Policy**

## **Incident Response Team**

| **Name** | **Role** | **Contact** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

## **Incident Response Workflow**

* The person who discovers the incident contacts the IT Manager.
* The following will be logged:
  + The name of the incident reporter.
  + Contact information of the incident reporter.
  + Time of the incident report.
  + The nature of the reported incident.
  + Involved equipment, software components, or persons.
  + Detection of the incident.
* An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

| **Security level** | **Description** | **Examples** |
| --- | --- | --- |
| Low or Medium Severity | Most issues fall under this category. These do not require someone to be paged or woken up in the middle of the night. | Suspicious emails, outages, strange activity on a laptop |
| High severity | These are problems where an adversary or active exploitation hasn’t been proven yet, and an attack may not have happened but is likely to happen. | Backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.) |
| Critical severity | The attackers were successful, and something was lost. |  |

* Incident Response Team establishes and follows procedures basing their response on the incident assessment.
* Incident Response Team does forensic analysis, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused.
* Incident Response Team restores the affected system(s).
* Incident Response Team assesses damage and cost.
* The affected clients are notified (if applicable).
* All incidents classified as “High” or above require a retrospective meeting and a “lessons learned” report.

## **Agenda of Response Meeting**

* Update the **Breach Timeline** with all known data related to the incident. The timeline should detail what you’re sure the attacker did at what times.
* Review new **Indicators of Compromise** with the entire group. Indicators of Compromise are anything you know belongs to the attacker: an IP address that sent data, a compromised account, a malicious file used to spearfish, etc.
* Update the list of **Emergency Mitigations**.
* Long Term Mitigations (including Root Cause Analysis): record everything you’ll start doing so this crisis doesn’t happen again.
* Everything Else: communications, legal issues, blog posts, status pages, etc.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by IT Manager.

# **Disciplinary Action**

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

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related documents**

* Backup Policy
* Business Continuity Plan
* Disaster Recovery Plan