***INJECT # - Incident Response Policy***

***Name of Company***

**Table of Contents**

[**Executive Summary** 2](#_Toc127449441)

[**Incident Response Plan** 3](#_Toc127449442)

[**Purpose:** 3](#_Toc127449443)

[**Scope:** 3](#_Toc127449444)

[**Roles and Responsibilities:** 3](#_Toc127449445)

[**Response Process:** 4](#_Toc127449446)

[**1.** **PREPARE** 4](#_Toc127449447)

[**2.** **DETECT** 5](#_Toc127449448)

[**3.** **ANALYZE** 5](#_Toc127449449)

[**4.** **RESPOND** 6](#_Toc127449450)

[**5.** **RECOVER** 7](#_Toc127449451)

[**6.** **REVIEW** 8](#_Toc127449452)

[**Incident Response Form** 9](#_Toc127449453)

[**References:** 10](#_Toc127449454)

[**Document History:** 10](#_Toc127449455)

# **Executive Summary**

This document covers an outline of …

# **Incident Response Plan**

## **Purpose:**

The purpose of this incident response policy is to provide an overview of procedures for responding to and managing incidents that may occur within the organization. The aim of incident response (IR) is to minimize the impact of an incident and return the organization to normal operations as quickly as possible.

## **Scope:**

This policy applies to all incidents that occur within the organization, regardless of the cause or severity. Incidents may include, but are not limited to:

* Cybersecurity breaches
* Natural disasters
* Power outages
* Hardware or software failures

## **Roles and Responsibilities:**

The [COMPANY NAME] roles and responsibilities diagram:

--Insert Diagram Here--

## **Response Process:**

For the most effective response, this incident response plan will be comprised of six stages: Prepare, Detect, Analyze, Respond, Recover, and Review. Each position of the InfoSec team will be designated a specific phase of the incident response plan that they are responsible for.

This incident response plan's effective implementation relies on the abovementioned roles. These roles will be expected to follow their specific duties, as the goals of each designated role are only attainable with reliance on the efforts and good works of others. Each stage also relies on strong communication of the details acquired from the completion of the previous stage.

#### **PREPARE**

The objective of the preparation stage is to position the InfoSec team in a manner that will allow them to respond to incidents quickly and effectively; while also hardening against future attacks. The preparation stage is the responsibility of the InfoSec Specialists and is comprised of the following steps:

* Incident Response Policy Creation/Auditing
  + Creating and maintaining IR policies, such as this one, are critical to effective incident response processes, and will be an ongoing process before and after incidents.
* Incident Response Training/Simulations
  + To ensure the effectiveness of IR policy, periodic training will be done to educate IT Security staff on policies in place, which will sometimes occur through incident simulations, coordinated by Information Security Specialists and the IT Security Lead.
* Incident Response Tools Research/Maintenance
  + Software and tools used throughout the IR process, such as forensic or deployment tools, must be actively maintained, with research regarding better alternatives also being conducted.
* Cybersecurity Policy Creation/Auditing
  + To reduce the potential attack surface that can result in an incident, the Information Security Specialists will also be responsible for creating and maintaining cybersecurity policies that enforces secure practices such as password requirements, acceptable use, BYOD, etc.

#### **DETECT**

The objective of the detection stage is to monitor different inputs of cyber information to detect potential intrusions as quickly and effectively as possible; to reduce dwell time in the event of a successful breach. This stage falls under the responsibility of our SOC Analysts, who will perform the following tasks:

* SIEM Management: Event Monitoring
  + The first step of detecting a potential incident will be the monitoring of log events recorded and reported by the SIEM in use, which the SOC analysts must then use to determine the severity of the event, resolving it themselves if not severe.
* Event Documentation
  + All events analyzed by SOC analysts must have the determined severity, cause, and remediation recorded in an organized manner, with escalations being recorded separately.
* Firewall/IDS Management
  + Along with information from the SIEM, SOC Analysts must also monitor and manage alerts from the firewall and IDS, recording severity, cause, and remediation for these events.
* Log Management
  + SOC Analysts must also manage logs, performing periodic audits of administrative systems, the SIEM logs, firewall logs, etc.

#### **ANALYZE**

The analysis stage begins once an event is escalated by a SOC Analyst, which then gets handled by a Cybersecurity Specialist. The Cybersecurity Specialist will then go through the following steps to determine if the event is a false positive, or if not, will determine the scope, impact, and origin of the incident.

* Incident Verification
  + In this step, it is up to the Cybersecurity Specialist to determine whether the escalated event is a false positive by verifying different details outlined in the SOC Analysts' report. If the event is not a false positive, it is declared an incident, and the IT Security team is notified.
* Scope Determination
  + Once an incident has been declared, the Cybersecurity Specialist will begin determining the scope of the incident by analyzing the type of attack and how it interacts with network architecture.
* Impact Triage
  + After the scope has been determined, the Cybersecurity Specialist will perform an impact triage to determine what systems are at the most risk and will require the most immediate attention.
* Log Analysis
  + Log analysis will be performed on the systems most at risk to determine if they have been affected by the incident and if so, the severity of its effects.

#### **RESPOND**

After the incident has been thoroughly analyzed, it is up to the Cybersecurity Specialist to perform the initial response to the incident, to contain the incident such that the threat actors perpetrating it are no longer an active threat to the organization. This phase includes the following steps:

* Exploit Sweep
  + Each system containing the vulnerability identified in the analysis stage must be documented for containment procedures to be effective. The response stage will begin with an exploit sweep that ensures all systems affected by the breach are correctly identified.
* Incident Containment
  + Once all affected systems have been identified, they can start becoming contained. This will look differently depending on the type of attack that occurred but will most commonly be resulted in removal from the active network.
* Access Management Control
  + If it is suspected that any type of access, such as administrative passwords, user IDs, and so on, has been compromised, an access management control lockdown will be implemented, resulting in more restrictive login requirements and possibly password resets.
* Evidence Preservation
* It is critical to preserve any evidence that may have been on systems during the incident to properly prosecute and investigate the incident after recovery and review. Effected systems that have been contained must be imaged so that investigation can take place without causing system modification.

#### **RECOVER**

The recovery phase's goal is to completely restore system operations so that regular business processes can resume, while also ensuring that the threat has been completely neutralized and hardening systems to reduce the likelihood of the same attack vector being used in the future. System Administrators will oversee the following tasks:

* Vulnerability Patching
  + Vulnerabilities discovered during the incident must be addressed as soon as possible, and if patching is not an option, workarounds must be implemented to ensure that the vulnerabilities do not pose a threat.
* System Hardening
* If the attack vector used to cause the breach does not involve any type of patching issue, systems must be hardened to prevent the attack vector that was used from being applicable in the future.
* Integrity Verification
* Once all systems are considered secure from the incident, integrity checks will be performed on various systems and their backups, ensuring that the threat actor had not been dwelling long enough to create a method of access that has been stored in backups.
* System/Backup Restoration
* Affected systems can now be restored to previous snapshots if required from damage caused, and restored systems can be put back into production environments after preliminary testing post-restoration.

#### **REVIEW**

The review phase serves to assess how effective and efficient the implementation of the IR plan was, to approve future applications of the IR plan, as well as reduce the overall risk of the organization. Information Security Specialists will be responsible for implementing the following steps in the review process:

* Incident Documentation
* The first step of an effective review process is to compile all information created or obtained regarding the incident, from every stage of the IR plan. A report will be generated detailing what information was learned at different stages, and what actions were taken based on the information gathered.
* Incident Response Effectiveness Documentation
* In a separate document, the effectiveness of each action taken at different steps of the response will be determined qualitatively, considering the specific person making the action and the information available. The overall effectiveness of the entire IR process against the threat contained will also be calculated.
* Incident Response Improvement Roadmap Creation
* After determining the effectiveness of the IR plan, a strategic roadmap will be created based on the deficiencies determined by the document on effectiveness that will outline the next steps to take to improve the IR process.
* Risk Mitigation
* A separate recommendation document will be created outlining the different non-IR areas that need to be improved for future risk mitigation, also using information gathered in the documents above.

**[ Insert Logo Here ]**

# **Incident Response Form**

**Incident Name:**

|  |
| --- |
| **General Information** |

Date and Time of the Incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Reported by:

|  |
| --- |
| **Incident Summary** |

Type of Incident Detected: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description of Incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Impact on Services | |
| Service: | Impact: |
|  |  |
|  |  |
| Impact on Information (Access logs, changes, deleting, etc.) | |
| Information: | Impact: |
|  |  |
|  |  |

# **References:**

EXAMPLE REFERENCE 1. (n.d.). *Scope of practice*. <https://www.nursingworld.org/practice-policy/scope-of-practice/>

EXAMPLE REFERENCE 2. (2020). *Publication manual of the American Psychological Association* (7th ed.). <https://doi.org/10.1037/0000165-000>

# **Document History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versions** | **Change Date** | **Responsible** | **Summary/Comments** |
| #-01 | 02/18/2023 | *Company Name* | This is the original version of the document set as a template. |
| #-01 | 02/18/2023 | *Company Name* |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |