<Business Name>

Incident Response Plan

Version 1.0

Revision History

|  |  |  |
| --- | --- | --- |
| Revision Date | Revision Made | Revision Author |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1. Introduction 4](#_Toc68473492)

[1.1 General Information 4](#_Toc68473493)

[1.2 Incident Response Plan Overview 4](#_Toc68473494)

[2. Team Structure 4](#_Toc68473495)

[2.1 Local Incident Response Teams 4](#_Toc68473496)

[3. Company Notification Policy 6](#_Toc68473497)

[3.1 Notification Process 6](#_Toc68473498)

[4. Initial Investigation 6](#_Toc68473499)

[5. Incident Responses 6](#_Toc68473500)

[5.1 DDoS 6](#_Toc68473501)

[5.2 Insider Threat 6](#_Toc68473502)

[5.3 Malware Infection 7](#_Toc68473503)

[5.4 Phishing 7](#_Toc68473504)

[5.5 Ransomware 7](#_Toc68473505)

# Introduction

## General Information

This document will discuss the steps to be taken for an incident response for the Cyber Security team. Mentioned will be points of contact, strategies, and policies to follow. This document is considered classified and confidential to within the <Team/Department Name> and should not be publicly displayed.

This document is not designed for how a general employee should proceed after finding an issue, but for the security team once the issue has been escalated to them. It is written in high level language and is not intended to be a technical how-to.

For information regarding this manual please contact: < Name, Email, Phone Number>

*This document is live and subject to change due to ongoing efforts to improve the integrity of the information systems of this company.*

## Incident Response Plan Overview

This incident management plan establishes the recommended actions, and procedures needed to

* Recognize and respond to an incident
* Assess the situation quickly and effectively
* Notify the appropriate individuals and organizations about the incident
* Organize the company’s response activities, including activating a command center
* Escalate the company’s response efforts based on the severity of the incident
* Support the business recovery efforts being made in the aftermath of the incident.

Existing incident management plans should conform to the Incident Management Policy statement found

This plan is designed to minimize operational and financial impacts of such a disaster and will be activated when a local Incident Manager or designated member determines that a disaster has occurred.

Specific details on incident response and subsequent business recovery actions and activities are included within the respective local recovery team plans.

# Team Structure

## Local Incident Response Teams

To successfully recover from a disaster total coordination of all incident management and recovery activities is needed. In a crisis, each team has specific functions that contribute to the success of the recovery. The following depicts the structure of a local incident management team, particularly in the aftermath of an incident. It is based on the Incident Command System (ICS).

Incident Command: <Employee Name>

Information Officer: <Employee Name>

Liaison Officer: <Employee Name>

Safety Officer: <Employee Name>

Logistics Section: <Employee Names>

Finance and Admin Section: <Employee Names>

Planning Section: <Employee Names>

Operation Section: <Employee Names>

<The teams listed below may be subject to change or merge due to existing team structures within the adopting company. It is however important to ensure these roles are all touched upon>

**Administration Team** will support the purchasing and evaluation of necessary tools for <Business Name>’s readiness to fight off and respond to incoming threats.

**Logistics Team** will support the necessary services to the incident response management and recovery efforts by communicating with necessary people, getting necessary information, or evaluating legal responsibilities in time of crisis.

**Operations Section** will support the necessary services for carrying out the actions outlined in this document.

**Planning Section** will support the upkeep of the Incident Response documentation along with the review of incidents to better improve <Business Name>’s response to information systems incidents.

<More teams and sections may be created due to the needs of the company>

# Company Notification Policy

## Notification Process

When notifying an affected employee or the company, the incident should be taken into consideration. For example, if the email system’s integrity has been broken, sending out a communication clip via email should not be avoided.

# Initial Investigation

The following questions should be recorded:

1. How was the incident discovered?
2. What is the category of the incident?
3. Where was the threat initiated? (Email, firewall, etc...)
4. What actions were immediately taken upon discovery?
5. Has the device been disconnected from the network?
6. What actions have been taken since discovery?

# Incident Responses

## DDoS

1. Containing the Incident
   1. Analyze the attack
      1. Determine the infrastructure components affected
      2. Determine the target. (Is it you or are your collator)
      3. Review logs to find the malicious traffic from the benign.
   2. Contact ISP for help in controlling traffic (Effective actions may only be able to be taken on their side)
   3. Determine if company received any threat prior to attack warning on incident
   4. If traffic is coming through a specific feature, disable it.
   5. Attempt to bottleneck or block the DDoS traffic as close to the cloud as possible.
   6. Cut unwanted connections on servers and routers.
      1. Configure their TCP/IP settings based off new information
   7. Set up/Use alternative communication means between the company and clients, end users.
2. Remediation
   1. Ensure ISP will enforce/block future attempts on the attack’s information.
   2. Take possible legal actions on responsible party.

## Insider Threat

1. If unconfirmed
   1. Begin forensics on the suspected insider threats devices
      1. Be sure to confiscate the devices without warning to prevent possible destruction of evidence.
   2. Log results
2. If already confirmed
   1. Report to legal team or law enforcement giving them all requested evidence. Be ready to help assist investigation

## Malware Infection

1. Containing the Incident
   1. Identify the system(s) affected
   2. Identify the data compromised
   3. Identify how the malware gained access to the machines / vulnerability exploited
   4. Remove the device from the network.
2. Remediation
   1. Clean the affected system(s) with malware removal tool
   2. Reattach the system(s) to the network
   3. Ensure antivirus software is up to data

## Phishing

1. Containing the Incident
   1. Once a malicious link/address has been discovered contact the operations team to block it via network wide. If this is not attainable, spread the malicious link/address and its meaning to ensure other employees will not be fooled.
2. Remediation
   1. If the employee clicked on any links have their desktop scanned for any malicious activity.
   2. If the employee entered any account information have the user change their credentials to protect their account.,
   3. Contact the compromised sender (If applicable) to ensure they are aware of the breach.

## Ransomware

1. Containing the Incident
   1. Disconnect infected computers from the network
   2. If isolation is not attainable, disconnect shared drives
   3. Block traffic that has been identified as communicating with the attacker
2. Remediation
   1. Attempt to regain control of device or files within the device
   2. If unsuccessful, reimage the affected devices with a clean install.
3. Recovery
   1. Before beginning to reconnect devices, ensure they are clean of malicious code.
   2. Monitor network to ensure there is not unusual, suspicious activity
   3. Restore possible data from employees’ backups (If attainable)