Heimdal®

Incident Management Policy Template

1. Introduction

This Incident Management Policy establishes the framework and guidelines for managing incidents that impact [Organization Name]'s information assets, systems, and operations.

It outlines the structured approach to effectively prepare for, respond to, mitigate, and recover from incidents to minimize their impact on business operations and ensure continuity.

2. Purpose

This policy establishes the requirements for reporting and managing incidents concerning {COMPANY-NAME}'s information systems and operational procedures.

It enables {COMPANY-NAME} to detect security incidents promptly, highlighting the importance of monitoring to mitigate potential damages effectively. Without such measures, the repercussions of an incident could be much more severe than if it were identified and addressed swiftly.

The scope of this policy encompasses all {COMPANY-NAME} information systems and components, specifically including:

- Centralized computing resources such as mainframes, servers, and similar devices.
- Storage solutions including devices for centralized data storage.
- Distributed computing devices like desktops, laptops, and similar technology.
- Networking equipment, including routers, switches, and other related devices.
- Security apparatus, such as firewalls, Intrusion Detection/Prevention (IDP) sensors, and similar devices dedicated to security functions.

3. Policy Overview

Computer Emergency Response Measures

Management at {COMPANY-NAME} is required to formulate, keep up to date, and periodically conduct tests on emergency response strategies.

These strategies should ensure the uninterrupted functioning of essential computing and communication systems in case there is a disruption or a decline in service quality, such as when Charter connectivity fails or a malware incident occurs in isolation.

Elements of the Incident Response Plan

The incident response strategy of {COMPANY-NAME} must delineate roles, duties, and strategies for communication following a security breach, including the process of informing pertinent external entities.

The plan should comprehensively address:

- Detailed procedures for responding to incidents;
- Strategies for business recovery and maintaining operations continuity;
- Processes for backing up data;
- Examination of legal obligations to report security breaches;
- Identification and safeguarding of all essential system components;
- Incorporation or reference to the incident response procedures of important external partners, such as payment card issuers and suppliers.

Incident Response Testing

The IT Department is required to conduct annual tests using simulated incidents to evaluate the effectiveness of their response. These tests may be combined with other related plan tests (e.g., Business Continuity Plan, Disaster Recovery Plan) when available. The outcomes of these tests will be recorded and shared with important stakeholders.

Incident Response and Recovery

A security incident response system will be established for all information systems managing or accessing information controlled by {COMPANY-NAME}. This system will feature a structured plan covering the seven phases of incident response:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activity

An incident response team will be designated to manage incident response tasks. This team will enact the incident response plan in the event of an incident. To ensure readiness, team members will undergo annual incident response training.

Additionally, incident response plans will be annually reviewed and updated as necessary, based on the findings from previous tests or real-world activations of the plan. Updated plans will then be disseminated to key stakeholders.

Mitigating Malicious Software

The approach to dealing with incidents involving malicious software will be tailored to the incident's extent and seriousness as assessed by the Information Security Management team. Potential actions include, but are not limited to, the use of one or more malware removal tools, isolating affected data, permanently erasing data, cleaning hard drives, or destroying the hard drives/media involved.

Handling Data Breaches

Management at {COMPANY-NAME} is tasked with developing, testing, and annually revising an Incident Response Plan. This plan should detail the policies and procedures to follow in the event that sensitive customer data is compromised.

Adapting the Incident Response Plan

The Incident Response Plan should be periodically updated to incorporate insights gained from handling real incidents and to stay current with industry advancements.

Program Communication

1. **Notification to external parties**

Reporting of information security breaches to external entities is not mandatory unless dictated by legal or regulatory requirements. The decision to disclose such incidents externally must be carefully considered by senior management, in collaboration with legal counsel, the Security Officer, and the IT Vice President, evaluating the benefits and drawbacks of making such disclosures.

In instances where a confirmed or highly probable security issue with information systems results in the exposure of private or confidential data of third parties to unauthorized individuals, it is imperative to promptly inform the affected parties about the breach.

Should sensitive data be lost or believed to have been accessed by unauthorized parties, immediate notification is required for both the data's Owner and the Security Officer.

2. **Information on Reporting Incidents**

{COMPANY-NAME} must ensure that details on how to report information security incidents are easily accessible and visible on common public communication platforms, including bulletin boards, break rooms, newsletters, and the company intranet.

3. **Informing Members**

The process of notifying members will be managed and executed by {COMPANY-NAME}'s Director of Risk Management. The notification must include, at the very least:

- Suggestions for members on how to safeguard themselves;
- Information on how to contact the Federal Trade Commission;
- Details on contacting the credit bureaus.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments

Sample Notification Letter

[Enter date here]

Dear [Enter member's name here],

At {COMPANY-NAME}, our priority is to promptly respond in the best interest of our members. We have recently identified an issue where certain members' confidential information was accessed without authorization. [Briefly outline the incident]

In response, we have implemented measures to secure our members' information and prevent further exposure. [Briefly describe the actions taken by {COMPANY-NAME}]

Due to this incident, there's a heightened risk of your personal information being misused for fraudulent activities. While it's difficult to predict if this will lead to any direct issues for you, we advise taking precautionary measures to safeguard your information. Here are some steps you can follow:

- Monitor your account statements closely. Should you notice any irregularities, please contact {COMPANY-NAME} immediately.
- For additional support and to report potential identity theft, you can reach out to the Federal Trade Commission (FTC) through their website or by calling their helpline.
- Visit ***http://www.ftc.gov/bcp/edu/microsites/idtheft/*** or call ***1-877-438-4338 (TTY: 1-866-653-4261).***