Document Name: [COMPANY] Incident Response Plan
Last Revision: [INSERT]
Next Revision: [INSERT]
Document Owner: [INSERT TEAM(S)]

[COMPANY] Incident Response Plan

Version 1.0

CONFIDENTIAL

Table of Contents

Introduction

At [COMPANY], we aim to handle any information security events quickly and efficiently. Our Incident Response Plan ensures that when things go wrong, we're ready to take the right steps to minimize damage to our business, our team, and the customers whose data we hold.

This plan helps us act in a way that protects the company and keeps everyone informed, ensuring the fastest possible recovery after an incident.

Definitions

Here are some of the terms we use in this plan to keep things clear:

Incident: Any event that disrupts our business operations, whether it affects a single person or the whole company. If it interrupts our ability to work, it's considered an incident.

Incident Management: The process of handling and fixing service disruptions as fast as possible to get us back to normal operations.

Personally Identifiable Information (PII): Information that can identify someone (like their name, ID number, or address).

Sensitive Personal Data: A special type of PII that can cause harm if exposed, such as health information or financial details.

Detection and Reporting

Whenever an issue is detected, the first step is to let the team know. At [COMPANY], we use email and [SLACK / MS TEAMS CHANNEL] to report potential security problems. We ask our team to act like a detective—describe the issue in detail, include what you've seen, and provide any evidence that can help us investigate the situation.

If you think something's wrong, report it immediately to [EMAIL] or [CHANNEL ID].

Roles and Responsibilities

At [COMPANY], we have clearly defined who is responsible for each part of the incident response process.

The Security Team or Designated Role(s):

- Respond promptly to any alerts or reports of potential incidents.
- Determine how severe the incident is (Low, Medium, High, or Critical).

- If necessary, take immediate steps to contain the issue and prevent further damage.
- Collect and preserve evidence to help with investigations.
- Document what happened, how it was handled, and what we learned for the future.

When Personal Data Is Involved:

- Notify executive management and anyone else on the team who needs to know (like legal or PR).

Communication:

- Ensure that relevant team members and any affected customers are notified promptly, meeting legal or contractual obligations.

Response Coordination

We use [SLACK / OTHER SYSTEM] to communicate and coordinate our responses during incidents. For High or Critical incidents, we set up a specific channel for the issue and include the relevant people, assigning roles as needed.

- Slack Channel: [CHANNEL LINK]
- Conference Call Number: [NUMBER AND MEETING ID]
- One-Click Join: [+PHONE NUMBER,,,MEETING ID#]

For high-priority issues, make sure to message the channel directly and notify key executives like the CEO and CTO until someone acknowledges the situation.

Internal Issues

Issues where the malicious actor is inside the company requires sensitive handling. Please contact the CEO directly and do not discuss with other employees. These are sensitive situations and must be handled appropriately.

Compromised Communications

If internal communication systems (such as Slack, email, or company phone systems) are compromised, we will use an alternate communication method to coordinate our response. The following steps will ensure we have a backup communication plan in place:

1. Set up alternate communication methods: Before an incident occurs, make sure your team has access to:
    a. Personal email accounts
    b. Personal phone numbers (preferably on a separate phone or device from the business)

    c. A messaging app like Signal or WhatsApp as a secondary option if company systems are compromised.
2. Predefined Backup Plan: If there's suspicion that internal communications are compromised, a designated person (e.g., CEO or IT Lead) will instruct the team to switch to the predefined alternate communication method. For example:
    a. Use a Signal group chat or personal email chain to continue coordination.

Incident Response Process

At [COMPANY], we follow a simple process to respond to any incidents. Here's how we do it:

Assign the Severity

We determine how severe the issue is using the following levels:

Severity Level	Description
Level 4: Critical	Exposure (or possible exposure) of sensitive personally identifiable information, which could put individuals at risk if disclosed. Examples include sexual orientation, genetic information, and so on.
Level 3: High	Exposure (or possible exposure) of personally identifiable information (PII), payment card information (PCI), protected health information (PHI), Controlled Unclassified Information (CUI), classified information, or other data that could lead to critical losses if disclosed or corrupted. Examples of "other data" could include client data, pricing models, secret recipes, and so on.
Level 2: Medium	Exposure (or possible exposure) of Confidential information that could result in a significant loss to the organization if lost or disclosed. Examples of confidential data could be business proposals, customer lists, HR files, student behavior reports, staff compensation, and financial reports.
Level 1: Low	An incident in which no data is exposed or possibly exposed or the only data exposed or possibly exposed is publicly available or of no value. Examples would be email address lists, training materials (if not confidential), press releases, and class schedules.

Take Action Based on Severity

Low/Medium Severity:

- Our team takes immediate steps to fix the problem and documents what happened. This might include resetting a password, updating software, or improving security settings.
- We record the issue and how it was resolved for future reference.

High/Critical Severity:

- We act fast to contain the problem. This might mean disconnecting affected systems, blocking suspicious accounts, or implementing emergency fixes.
- We immediately notify key stakeholders, including executives, legal teams, and customers, to meet any legal or contractual obligations.
- A special War Room is created for communication and updates during the incident. This includes regular meetings to discuss:
    - Timeline updates
    - New evidence or indicators of compromise
    - Emergency mitigation measures
    - Long-term solutions to prevent the issue from happening again

Investigate and Remediate

We investigate the root cause of the incident, gather any necessary evidence, and fix the problem. This includes reviewing security settings, patching vulnerabilities, and working with external experts if needed.

Post-Incident Review (Post-Mortem)

Once the incident is resolved, we don't stop there. We review the incident to learn from it and improve our processes:

- Document the Incident: We write down everything we learned, including what happened, how we fixed it, and what could have been done better.
- Team Review: We hold a quick meeting to go over the incident, discuss what worked well, and identify areas for improvement.
- Action Items: Any follow-up tasks are assigned to specific team members to ensure we're better prepared next time.

Long-Term Fixes

Based on what we learned, we implement long-term solutions to prevent the incident from happening again. This might include:

- Installing new security software.
- Updating our incident response processes.
- Providing additional training to employees on security best practices.

Runbooks

For specific types of incidents, we may create Runbooks—detailed instructions on how to handle common issues. For now, we focus on the basics, but as we continue to expand our program, we'll develop and include these step-by-step guides to make our response even faster and more efficient.

Appendix A: Revision History

This is a controlled document. This section highlights major and minor changes to the document as it is revised.

Revision	Date	Description	Approved by
1.0		Initial Version	