Cybersecurity Incident Response Plan Template

Document version: [Version Number]
Date of issue: [Issue Date]
Next scheduled review: [Date]

Introduction

This Cybersecurity Incident Response Plan template is provided as a foundational framework by [Company-Name], intended for use by organizations seeking to establish a robust, structured, and effective approach to managing cybersecurity incidents.

This template is to empower organizations to develop a comprehensive incident response strategy that aligns with their specific operational needs, threat landscapes, and compliance obligations.

Purpose

The purpose of this IRP is to ensure that the organization can promptly and effectively respond to various cybersecurity incidents, minimize damage and recovery time, and mitigate the risks associated with such incidents.

Scope

This plan applies to all information systems, network infrastructure, and data processed, stored, or transmitted by the organization, including data held on behalf of third parties.

Incident Response Phases

1. **Preparation**

Develop and maintain incident response policies and procedures.	Done
Conduct regular training and awareness sessions for the IRT and staff.	Done
Establish communication plans and channels.	Done

2. **Identification**

Monitor systems and networks for signs of a security incident.	Done
Develop criteria for incident classification and severity levels.	Done
Utilize tools and processes for effective detection and analysis.	Done

3. **Containment**

Short-term: Isolate affected systems to prevent further damage.	Done
Long-term: Implement measures to secure network segments and systems.	Done

4. **Eradication**

Remove the cause and sources of the incident.	Done
Securely wipe affected systems and verify the integrity of backups before restoration.	Done

5. **Recovery**

Restore systems and services from clean backups.	Done
Monitor for signs of malicious activity to ensure that the threat is completely removed.	Done
Gradually return operations to normal.	Done

6. **Lessons Learned**

Conduct a post-incident review to identify strengths and weaknesses in the response process.	Done
Document findings and implement improvements to the IRP and security posture.	Done

7. **Communication Plan**

Define protocols for internal and external communications during an incident.	Done
Identify key contacts within the organization and external stakeholders, such as law enforcement and regulatory bodies.	Done

8. **Review and Maintenance**

Regularly review and update the IRP to reflect changes in the threat landscape, organizational structure, and technological environment.	Done
Conduct periodic drills and simulations to test the effectiveness of the plan.	Done

Annexes

- Incident Response Checklists
- Contact Lists for IRT and Key Stakeholders
- Templates for Communication (internal alerts, public statements, etc.)
- Legal and Regulatory Compliance Requirements

Document Control

Version: [version number]

Last Reviewed: [date]

Next Review Date: [date]
Owner: [owner's name & department]