Incident Response Plan Template

1. Incident Identification:

Description of the Incident:

[Briefly describe the nature of the incident]

Date/Time of Detection:

[MM/DD/YYYY, HH:MM]

Detection Method:

[How was the incident detected?]

Initial Reporter:

[Name/Role of the person who reported the incident]

2. Incident Classification:

Severity Level:

[Low/Medium/High/Critical]

Type of Incident:

[e.g., Data Breach, Unauthorized Access, Malware, DDoS Attack]

Affected Systems:

[List the affected systems or networks]

3. Incident Response Team:

Incident Lead:

[Name/Role]

Team Members:

[Names/Roles of response team members]

External Contacts:

[Law enforcement, Legal counsel, External cybersecurity services]

4. Immediate Response Actions:

Containment Strategy:

[Steps taken to isolate and contain the incident]

Preservation of Evidence:

[Methods used to preserve evidence (logs, system images, etc.)]

5. Investigation and Analysis:

Data Collection:

[Information and data collected during the investigation]

Analysis of Incident:

[Results of the analysis, including suspected cause and scope of impact]

6. Eradication and Recovery:

Eradication Measures:

[Actions taken to remove the threat or vulnerability]

Recovery Process:

[Steps to restore systems and services to normal operation]

7. Post-Incident Activities:

Lessons Learned:

[Summary of what was learned from the incident]

Post-Incident Report:

[Detailed report including timeline, impact assessment, response effectiveness]

Improvements:

[Recommended changes to prevent similar incidents or improve response]

Incident ID	Incident Classification	Incident Response Team	Immediate Response Actions	Investigation and Analysis	Eradication and Recovery	Post-Incident Activities