Incident Response Plan Template

Introduction

Purpose: Define the purpose of the incident response plan.

Scope: What incidents it covers (data breaches, malware, insider threats).

Key Principles: Incident response should be rapid, structured, and consistent.

Incident Response Phases

Each phase of the incident response process is critical and should be followed to ensure a timely and effective response.

1. Preparation

Objective: Set up the tools, team, and procedures to handle incidents.

Action:

- Establish an incident response team (IRT).
- Ensure security tools are in place (e.g., IDS/IPS, SIEM).
- Create an inventory of assets, networks, and data.

2. Identification

Objective: Recognize and confirm that an incident has occurred.

Action:

- Review alerts from monitoring systems.
- Determine if the event is a security incident or a false alarm.

- Categorize the type of incident (data breach, malware, insider threat, etc.).

3. Containment

Objective: Limit the impact of the incident.

Action:

- Short-term containment: Stop the spread of malware, isolate infected systems.

- Long-term containment: Prevent further damage while maintaining business continuity.

4. Eradication

Objective: Remove the cause of the incident from the network.

Action:

- Remove malware or compromised accounts.

- Patch vulnerabilities.

5. Recovery

Objective: Return affected systems to normal operations.

Action:

- Restore from backups.

- Monitor systems for any signs of lingering threats.

6. Lessons Learned

Objective: Review and improve the incident response process.

Action:

- Conduct a post-mortem analysis.

- Update response protocols and procedures based on the findings.