Incident Response Plan Template

Organization: ___________________________________

Date: ___________________________________

1. Purpose

This Incident Response Plan (IRP) establishes procedures to identify, respond to, and recover from information security incidents.

2. Scope

Applies to all employees, contractors, and systems within the organization's information technology environment.

3. Incident Response Team

Role	Name	Contact	Responsibilities
Incident Response Lead			
IT/Security Analyst			
Communications Coordinator			
Legal/Compliance Advisor			

4. Incident Categories

- Unauthorized Access
- Malware Infection
- Denial of Service (DoS/DDoS)
- Data Breach/Leak
- Physical Security Breach
- Other (Specify): ________________________

5. Incident Response Process

1. **Preparation**
    - Maintain contacts, tools, and documentation.
    - User awareness and training.

2. **Identification**
    - Detect and report potential incidents.
    - Validate authenticity and scope.

3. **Containment**
    - Short-term: isolate affected assets.
    - Long-term: implement temporary fixes.

4. **Eradication**
    - Remove threats and prevent recurrence.

5. **Recovery**
    - Restore affected systems and services.
    - Monitor for further anomalies.

6. **Lessons Learned**
    - Document findings and improve controls.

6. Incident Reporting

Report incidents to:
Email: ________________________
Phone: ________________________

7. Communication Plan

- Internal notifications (team, management)
- External notifications (customers, regulators as applicable)
- Approved public statements

8. Documentation

- Incident description
- Timeline of events
- Actions taken
- Root cause analysis
- Post-incident recommendations

9. Review and Update

- Review this plan annually or after significant incidents
- Record of last review: ________________________
- Next scheduled review: ________________________