RESILIENTLY

Cybersecurity made clear.

Incident Response Plan

A comprehensive framework for detecting, responding to, and recovering from cybersecurity incidents.

Free Template from Resiliently

resiliently.co/tools/templates

Version 1.0 | May 2026

1. Plan Overview

This Incident Response Plan (IRP) establishes the procedures and responsibilities for responding to cybersecurity incidents. It is designed to minimize damage, reduce recovery time, and protect organizational assets.

This plan should be reviewed and updated at least annually, or after any significant incident or organizational change.

Organization Name

Plan Owner/Author

Last Review Date

Next Review Date

2. Incident Response Team

The Incident Response Team (IRT) is responsible for coordinating the response to all security incidents. Team members should be trained on their roles and have 24/7 contact availability.

Role	Name	Primary Contact	Backup Contact

3. Incident Classification

Incidents are classified by severity to determine appropriate response levels and escalation requirements.

Severity Level 1 - Critical

Active breach with data exfiltration, ransomware deployment, or system-wide compromise. Requires immediate executive notification and potential law enforcement involvement.

Severity Level 2 - High

Confirmed intrusion or malware infection with potential for spread. Requires immediate IRT activation and stakeholder notification within 4 hours.

Severity Level 3 - Medium

Suspicious activity requiring investigation. May include failed attack attempts, policy violations, or anomalous behavior. Response within 24 hours.

Severity Level 4 - Low

Minor security events such as spam, phishing attempts blocked by controls, or routine policy exceptions. Standard ticketing and response.

4. Detection & Analysis

- [ ] Monitor security alerts from SIEM, EDR, and network tools
- [ ] Document initial indicators of compromise (IOCs)
- [ ] Determine scope of affected systems and data
- [ ] Preserve evidence for forensic analysis
- [ ] Classify incident severity level
- [ ] Notify appropriate team members based on severity

Detection Source

Initial IOCs Observed

Affected Systems/Assets

5. Containment Procedures

The goal of containment is to limit the scope and impact of the incident while preserving evidence for investigation.

Short-term Containment

- [ ] Isolate affected systems from the network
- [ ] Block malicious IP addresses and domains
- [ ] Disable compromised user accounts

- [ ] Capture volatile memory and system state
- [ ] Document all containment actions with timestamps

Long-term Containment

- [ ] Rebuild affected systems on clean infrastructure
- [ ] Apply emergency patches and security updates
- [ ] Enhance monitoring on affected network segments
- [ ] Implement additional access controls as needed

6. Eradication & Recovery

- [ ] Remove malware and attacker tools from all systems
- [ ] Reset credentials for all affected accounts
- [ ] Patch vulnerabilities exploited in the attack
- [ ] Restore systems from verified clean backups
- [ ] Verify system integrity before returning to production
- [ ] Monitor recovered systems for signs of persistence

Recovery Actions Taken

Systems Restored (with dates)

7. Communication Plan

Clear communication is critical during incident response. Use these guidelines for internal and external communications.

Stakeholder	Contact Method	Notification Timing	Responsible Party

8. Post-Incident Review

Conduct a post-incident review within 2 weeks of incident closure. Document lessons learned and improvement actions.

Incident Summary

Root Cause Analysis

What Worked Well

Areas for Improvement

Action Items