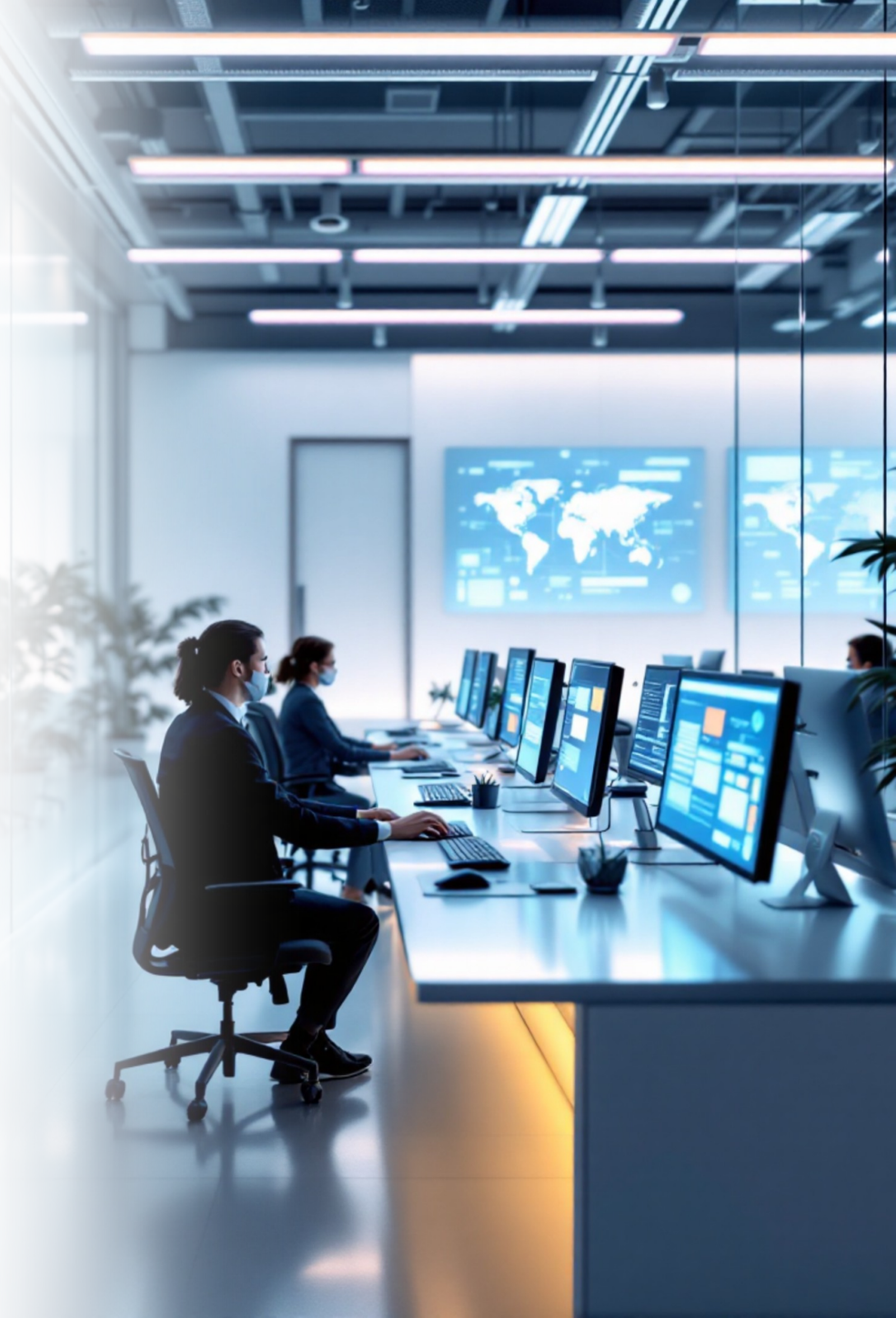
CSNP
CYBERSECURITY NON-PROFIT

Incident Response Plan Template

A comprehensive framework for preparing, detecting, and responding to security incidents. Designed for small to medium businesses and nonprofits by the Cybersecurity Non-Profit.



OVERVIEW

Understanding Your Incident Response Plan

What is an IRP?

An Incident Response Plan is your organization's documented approach to detecting, responding to, and recovering from cybersecurity incidents. It minimizes damage, reduces recovery time, and ensures coordinated action during critical moments.

Why You Need One

- Reduces response time from hours to minutes
- Minimizes financial and reputational damage
- Ensures regulatory compliance
- Protects customer data and trust

TEAM STRUCTURE

Incident Response Team Roles

Incident Commander

Leads response efforts, makes critical decisions, coordinates all team activities and communications

Security Analyst

Investigates incidents, analyzes logs, identifies attack vectors and assesses technical impact

Communications Lead

Manages internal and external communications, coordinates with PR and legal teams

Legal Advisor

Ensures compliance with regulations, advises on notification requirements and liability issues

Customize these roles based on your organization's size. In smaller teams, one person may fulfill multiple roles.

Incident Classification Framework

Properly classifying incidents ensures appropriate response levels and resource allocation. Use this matrix to categorize incidents by severity and impact.

Severity	Impact	Response Time	Example
Critical	Organization-wide	Immediate	Ransomware outbreak
High	Multiple systems	Within 1 hour	Data breach detected
Medium	Single system	Within 4 hours	Malware on workstation
Low	Minimal impact	Within 24 hours	Phishing attempt blocked

DETECTION

Detection and Identification

01

Monitor Security Tools

Continuously monitor firewalls, antivirus, intrusion detection systems, and SIEM alerts

02

Validate the Alert

Distinguish between false positives and genuine incidents through investigation

03

Document Initial Findings

Record time of detection, affected systems, and preliminary scope in incident log

04

Classify Severity

Apply classification framework to determine response priority and resources needed

05

Activate Response Team

Notify appropriate team members based on severity level and incident type

Containment Procedures

Quick Containment Actions

Time is critical. These immediate steps prevent incident spread while preserving evidence for investigation.

Always balance containment speed with evidence preservation needs. Document every action taken.

Isolate Affected Systems

- Disconnect from network
- Disable wireless connections
- Block compromised accounts

Prevent Lateral Movement

- Segment network traffic
- Update firewall rules
- Change administrative passwords

Preserve Evidence

- Capture system memory
- Clone affected drives
- Collect and secure logs

ERADICATION

Eradication Steps

Remove the threat completely from your environment. Rushing this phase can lead to reinfection.

Identify Root Cause

Determine how the attacker gained access and what vulnerabilities were exploited

Remove Malicious Components

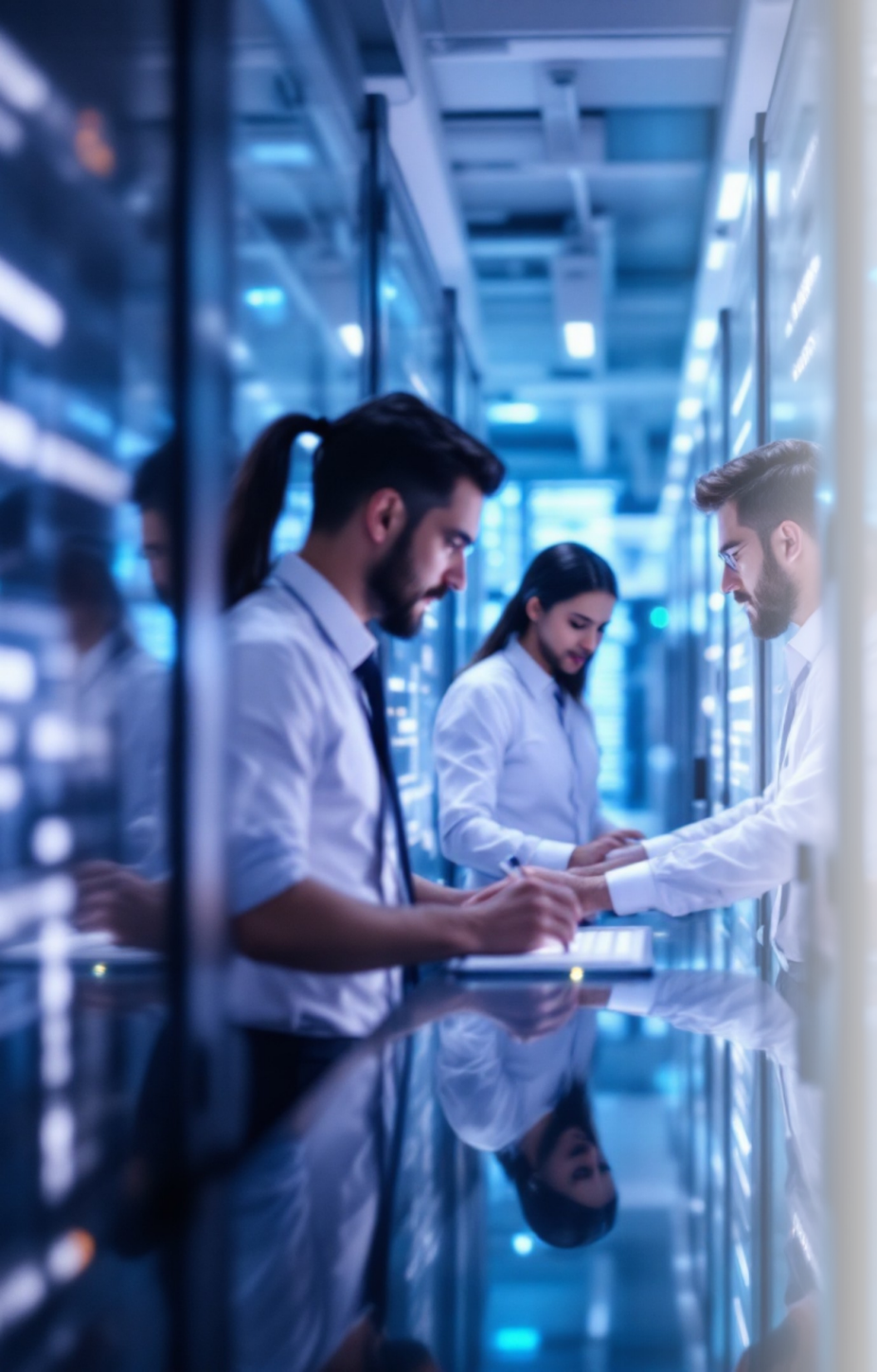
Delete malware, backdoors, unauthorized accounts, and any attacker-installed tools

Patch Vulnerabilities

Apply security updates, fix misconfigurations, and strengthen access controls

Verify Complete Removal

Scan systems thoroughly to confirm no trace of the threat remains before recovery



Recovery Procedures

Restore Systems

- Restore from clean backups
- Rebuild compromised systems
- Reinstall applications
- Restore data carefully

Validate Operations

- Test system functionality
- Monitor for suspicious activity
- Verify data integrity
- Confirm security controls

Return to Normal

- Gradually restore services
- Resume business operations
- Continue enhanced monitoring
- Update stakeholders

COMMUNICATION

Communication Plan

1

Internal Notification

Alert executive leadership, IT staff, and affected departments immediately. Use secure communication channels.

2

Customer Communication

Notify affected customers within required timeframes. Be transparent about impact and protective measures.

3

Regulatory Reporting

File required notifications with regulatory bodies, law enforcement, and industry partners as mandated.

4

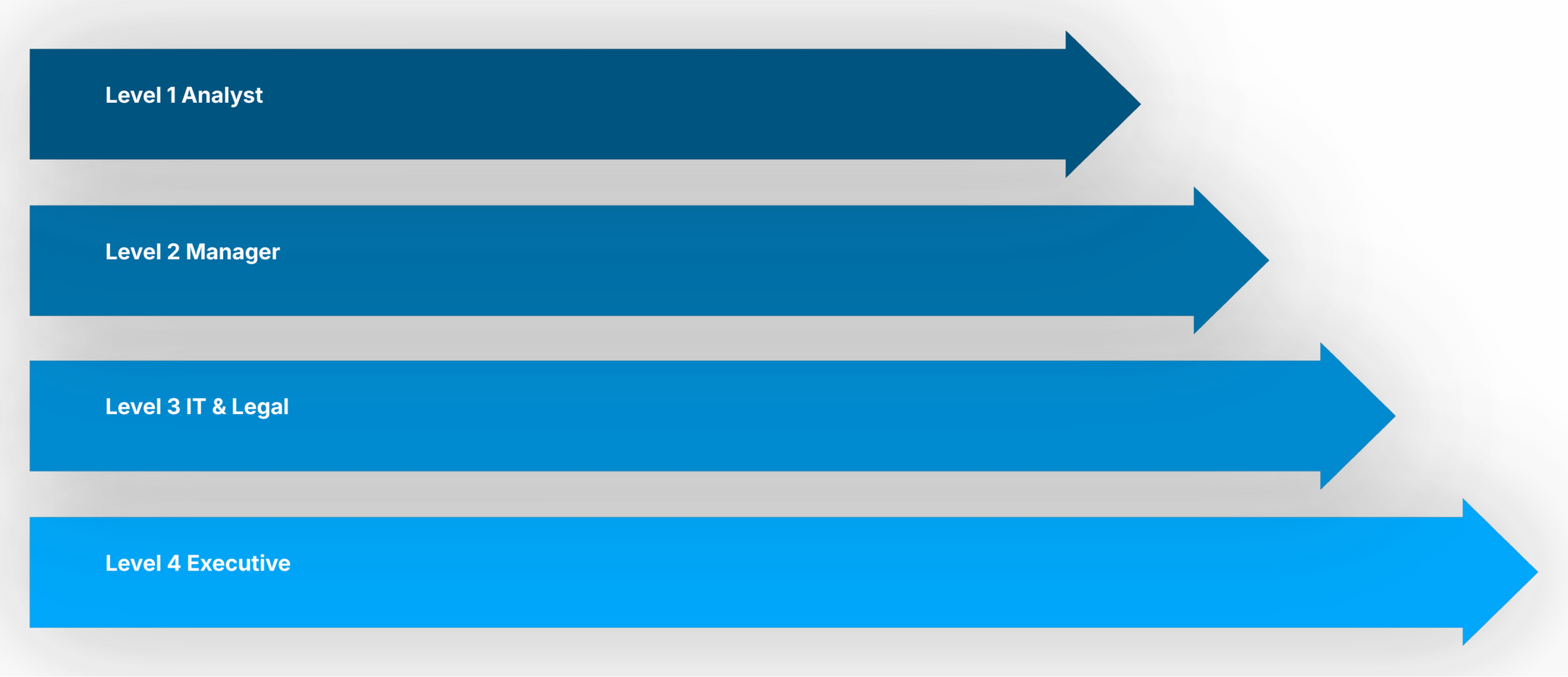
Public Relations

Coordinate media responses with PR team. Maintain consistent messaging across all channels.

Template: Draft pre-approved communication templates for common incident types to accelerate response time.

Escalation Matrix

Clear escalation paths ensure incidents reach the right decision-makers quickly. Customize this matrix for your organization's structure.



External Notification Requirements

Who to Notify

- **Law Enforcement**

  FBI, local cybercrime units for criminal investigations

- **Regulatory Bodies**

  State attorneys general, industry regulators, data protection authorities

- **Affected Parties**

  Customers, vendors, partners whose data may be compromised

- **Insurance Provider**

  Cyber insurance carrier for coverage and guidance

Notification Timelines

Jurisdiction	Timeframe
GDPR (EU)	72 hours
HIPAA (US Healthcare)	60 days
State Laws	Varies by state
PCI DSS	Immediately

Consult legal counsel to ensure compliance with all applicable regulations in your jurisdiction.

DOCUMENTATION

Evidence Preservation

Chain of Custody

Document who collected evidence, when, where, and how it was stored. Maintain detailed logs of all handlers and transfers to ensure legal admissibility.

Secure Storage

Store evidence in encrypted, access-controlled locations. Use write-protected media and maintain both physical and digital security controls.

Forensic Copies

Create bit-by-bit copies of affected systems before remediation. Use forensically sound tools and document hash values for integrity verification.

Post-Incident Review

Learning from incidents strengthens your security posture. Conduct a thorough review within one week of incident closure.

Timeline Analysis

Create detailed timeline from initial compromise to resolution. Identify detection delays and response bottlenecks.

Response Effectiveness

Evaluate what worked well and what didn't. Assess team coordination, tool effectiveness, and decision-making processes.

Root Cause Identification

Determine how the incident occurred and why existing controls failed. Look beyond immediate causes to systemic issues.

Improvement Actions

Document specific, actionable improvements to prevent recurrence. Assign owners and deadlines for each action item.

TEMPLATES

Essential Templates for Your Plan

Contact Lists Template

Role	Information Needed
Internal Team	Name, Title, Phone, Email, Backup
External Contacts	Organization, Contact, After-hours
Vendors	Service, Contact, Support Number
Legal/Regulatory	Agency, Requirements, Contact

Incident Log Template

Field	Details to Record
Date/Time	When incident occurred/detected
Type	Classification and severity level
Actions	All response steps taken
Impact	Systems, data, operations affected

Download customizable versions of all templates at csnp.org/resources

Plan Maintenance Schedule

Monthly

- Review and update contact lists
- Check backup restoration procedures

Semi-Annually

- Run full response simulation
- Update procedures and templates
- Provide team training

1 2 3 4

Quarterly

- Conduct tabletop exercises
- Update threat intelligence
- Review incident trends

Annually

- Complete comprehensive plan review
- Update based on new threats
- Executive leadership briefing

An outdated plan is as dangerous as no plan. Schedule these maintenance activities in advance and treat them as non-negotiable commitments.

About Cybersecurity Non-Profit (CSNP)

> *Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.*

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety Online
- Senior Digital Safety
- Women's Security Awareness
- Parents & Educators Resources

Free Resources

Everything we offer is completely free because we believe cybersecurity education should be accessible to all organizations and individuals, regardless of budget.

Visit us: csnp.org

Resources: csnp.org/resources