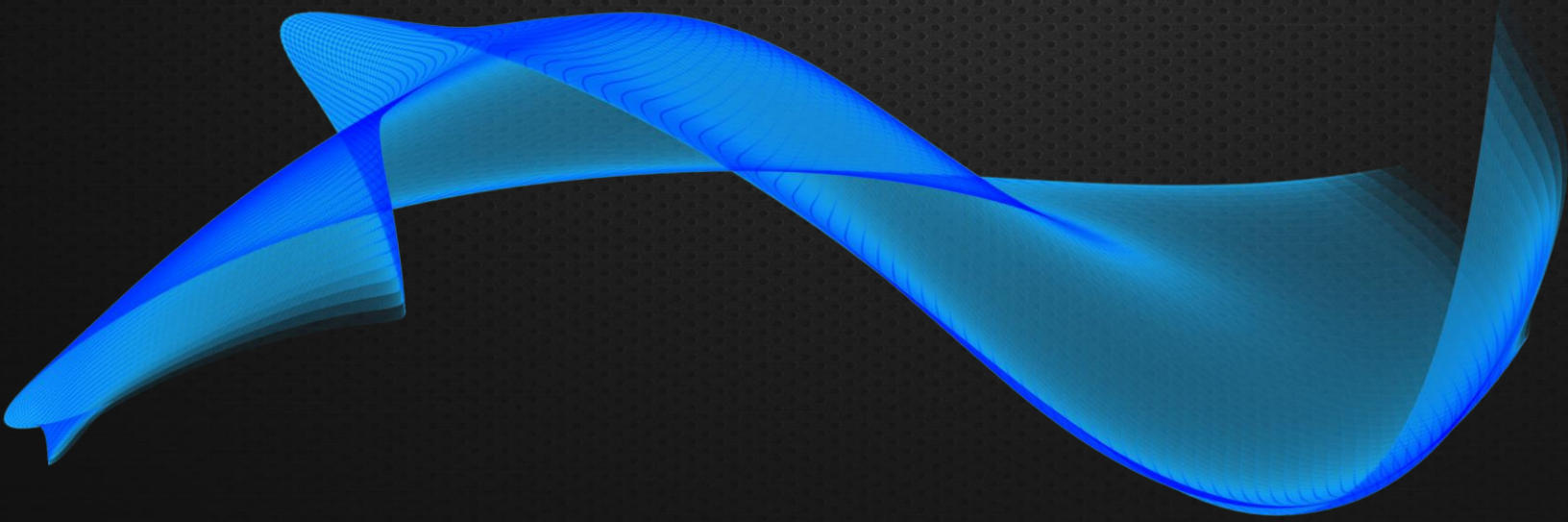
<PlaceYourCompanyNameHere>

Incident Response Plan



[Company Name]

Incident Response Plan (IRP)

Version: 1.0

Effective Date: [Insert Date]

Approved By: Executive Director / Board of Directors

---

1. PURPOSE

The purpose of this Incident Response Plan (IRP) is to establish procedures for identifying, responding to, mitigating, and recovering from cybersecurity incidents that threaten the confidentiality, integrity, or availability of [Organization Name]'s systems and data.

This plan ensures:

- Rapid containment of security threats
- Protection of client, donor, and employee information
- Compliance with regulatory and grant obligations
- Clear internal and external communication
- Business continuity

---

2. SCOPE

This plan applies to:

- All employees
- Volunteers
- Board members
- Contractors
- IT service providers
- Third-party vendors
-

It covers incidents affecting:

- Email systems
- Cloud platforms
- Servers and networks
- End-user devices
- Donor databases
- Financial systems
- VoIP systems
- Website infrastructure

3. DEFINITION OF A SECURITY INCIDENT

A security incident includes, but is not limited to:

- Ransomware attack
- Phishing compromise
- Unauthorized system access
- Data breach
- Malware infection
- Loss or theft of device containing sensitive data
- Denial-of-service attack
- Cloud account compromise
- Insider misuse

4. INCIDENT RESPONSE TEAM (IRT)

The following individuals are responsible for incident management:

Incident Lead:

Name: _____
Title: _____
Phone: _____

IT Support / MSP:

Company: _____
Contact: _____

Executive Oversight:

Executive Director: _____

Legal Counsel:

Contact: _____

Cyber Insurance Provider:

Policy #: _____

Claims Contact: _____

---

5. INCIDENT SEVERITY LEVELS

Level 1 – Low Impact

- Minor malware detection
- Phishing email blocked
- No confirmed data exposure

Level 2 – Moderate Impact

- Confirmed compromised account
- Limited data exposure
- Temporary service disruption

Level 3 – High Impact / Critical

- Ransomware
- Confirmed data breach
- Large-scale system compromise
- Regulatory reporting required

---

6. INCIDENT RESPONSE PHASES

PHASE 1: Identification

When an incident is suspected:

- ☐ Document date and time discovered
- ☐ Identify who discovered the issue
- ☐ Capture screenshots (if applicable)
- ☐ Do NOT power off device unless instructed
- ☐ Immediately notify Incident Lead

Initial Documentation:

Incident Description:

Systems Affected:

PHASE 2: Containment

Immediate actions may include:

- ☐ Disable compromised accounts
- ☐ Disconnect affected device from network
- ☐ Block malicious IP addresses
- ☐ Change passwords organization-wide (if required)
- ☐ Engage IT provider

Goal: Prevent spread of attack.

PHASE 3: Investigation

The Incident Response Team shall:

- [ ] Determine root cause
- [ ] Identify systems accessed
- [ ] Identify data exposed
- [ ] Preserve logs and evidence
- [ ] Determine attacker persistence

If cyber insurance exists:

- [ ] Notify insurance carrier before forensic action (if required by policy)

PHASE 4: Eradication

- [ ] Remove malware
- [ ] Patch vulnerabilities
- [ ] Reset credentials
- [ ] Remove unauthorized accounts
- [ ] Apply system updates

PHASE 5: Recovery

- [ ] Restore systems from clean backups
- [ ] Monitor systems for unusual activity
- [ ] Validate system integrity
- [ ] Confirm operations restored

PHASE 6: Notification & Compliance

If data breach is confirmed:

- [ ] Determine type of data exposed (PII, PHI, PCI)
- [ ] Consult legal counsel
- [ ] Notify regulatory bodies (if required)
- [ ] Notify affected individuals (if required)
- [ ] Notify grantor/funding agencies (if applicable)
- [ ] Notify Board of Directors

---

7. COMMUNICATION PLAN

Internal Communication

- ☐ Staff notified appropriately
- ☐ Board notified (if significant)
- ☐ Limit unnecessary disclosure

External Communication

Spokesperson: _____

All external communication must be approved by:

- ☐ Executive Director
- ☐ Legal Counsel

Public Statement Template:

"[Organization Name] recently identified a cybersecurity incident affecting certain systems. We immediately took steps to secure our environment and are working with experts to investigate. Protecting our community's information is a top priority."

---

8. DOCUMENTATION & EVIDENCE PRESERVATION

The following must be preserved:

- ☐ Log files
- ☐ Email headers
- ☐ Firewall logs
- ☐ Affected device images (if applicable)
- ☐ Timeline documentation

Maintain chain of custody if legal investigation possible.

---

9. POST-INCIDENT REVIEW

Within 30 days of resolution:

- ☐ Conduct internal debrief
- ☐ Document root cause
- ☐ Identify policy gaps

- [ ] Update cybersecurity controls
- [ ] Report summary to Board

Post-Incident Summary:

Incident Date:
Severity Level:
Root Cause:
Data Impacted:
Corrective Actions:

---

10. BUSINESS CONTINUITY CONSIDERATIONS

If operations are disrupted:

- [ ] Activate backup communication methods
- [ ] Shift to manual operations if needed
- [ ] Use alternate systems
- [ ] Prioritize critical services

---

11. TESTING & MAINTENANCE

This Incident Response Plan shall be:

- [ ] Reviewed annually
- [ ] Tested via tabletop exercise annually
- [ ] Updated after major incidents

Employee Reporting Requirement

All staff must report suspected incidents immediately to:

[redacted]

Failure to report suspected incidents may increase risk and liability.

Acknowledgment

I acknowledge that I understand the Incident Response Plan and agree to follow reporting procedures.

Name:
Signature:
Date: