Comprehensive Incident Response Plan

[NAME OF ORGANIZATION]

Effective Date: [Date]

Policy Owner: [Insert Name]

Last Updated: [Date]

Review Date: [Annual Review Date]

IMPORTANT: Print this document and store it in a safe physical location. During an incident, you may not be able to access the digital version.

EMERGENCY CONTACT AND COMMUNICATION SHEET

Print this section and keep it accessible for immediate response. Use when you need to act quickly during an emergency.

[ ] Set up a Signal group for your core response team.

Fill in contact details below:

Role	**Contact Information (Name/Phone/Signal)**
Incident Lead	Name: _____ Phone: _____ Signal: _____ *Responsibilities: Overall coordination, external communications authorization, resource allocation*

Technical Lead	Name: _____ Phone: _____ Signal: _____ *Responsibilities: System analysis, containment, evidence collection, recovery planning*
Communications Lead	Name: _____ Phone: _____ Signal: _____ *Responsibilities: Media relations, staff notifications, stakeholder updates*
Legal Contact	Name: _____ Phone: _____ Available hours: _____ *Responsibilities: Law enforcement coordination, legal compliance, breach notification requirements*
Executive Contact	Name: _____ Phone: _____ Signal: _____ *Responsibilities: Final decisions and authorization*
Support Coordinator	Name: _____ Phone: _____ Signal: _____ *Responsibilities: Staff wellbeing, mental health support, community impact assessment*

External Support Contacts:

Technical Support	Company: Point of Contact: Phone:

Groundwire Team	Groundwire Advisors Josh: josh@groundwireadvisors.com Signal Galia: galia@groundwireadvisors.com Signal: @galiaN.07 help@groundwireadvisors.com Response time: Within 24 hours
Law Enforcement	Local Police: [Phone Number] Local FBI Office: [Phone Number] *It's preferable to include a cyber-specialize team, if there is one in your area.*
Cyber Insurance	Company: [Name] Phone: [Phone Number]
Mental Health	Provider: [Name] Crisis line: [Phone Number]

Communication Protocols During an Incident

Internal Communications During Incidents

[ ] Secure channel activated - Switch to Signal/encrypted email

[ ] Key staff notified within 30 minutes

[ ] All staff briefed within 2 hours (use secure methods)

[ ] Regular updates established (every 2-4 hours during active incident)

[ ] Clear guidance provided on what staff should/shouldn't do

External Communications Guidelines

Key principles:

- All external communications must be approved by Incident Commander
- Be transparent but protect sensitive details
- Coordinate with legal counsel before public statements
- Prioritize affected individuals in notifications
- Follow legal notification timelines strictly

Media Relations

If media contact occurs:

[ ] Refer all media inquiries to Communications Lead

[ ] Prepare holding statement if needed

[ ] Coordinate response with legal counsel

[ ] Document all media interactions

DETAILED INCIDENT RESPONSE PLAN

This section provides comprehensive checklists and procedures for each phase of incident response. Use this for detailed guidance during and after an incident.

Phase 1: Stop the Damage (First 30 Minutes)

The first priority is to prevent the incident from getting worse. Act quickly but deliberately.

Immediate Actions Checklist

[ ] STOP - Don't continue using compromised accounts/systems

[ ] Disconnect affected devices from internet immediately

[ ] Assess safety - Is there immediate physical threat to staff?

[ ] Document everything - Screenshot with timestamps before systems change

[ ] Preserve evidence - Don't delete anything, even if embarrassing

[ ] Change passwords on affected accounts from a clean device

[ ] If you don't know which accounts, change all passwords

[ ] Activate secure communications - Switch to Signal/encrypted channels

[ ] Alert incident lead - Contact primary incident responder immediately

[ ] Brief assessment - What type of incident appears to be occurring?

Special Considerations

If data was shared accidentally:

[ ] Contact recipients to request deletion

[ ] Document who received the data and when

If physical theft:

[ ] Report to local police immediately

[ ] Change passwords for any accounts accessible from stolen device

[ ] Enable remote wipe if possible

For personal targeting/harassment:

[ ] Screenshot all threats with full URLs and timestamps

[ ] Don't engage with attackers on social media or email

[ ] Check data broker sites for your personal information

[ ] Consider temporary social media break if harassment is ongoing

Initial Notifications (Within 1 Hour)

[ ] Incident lead notified

[ ] Technical support contacted (if needed)

[ ] Legal counsel alerted (if sensitive data involved)

[ ] Executive director/senior leadership informed

[ ] Key staff who need to know immediately informed

[ ] All staff briefed (use secure methods, not compromised email)

Phase 2: Document Everything (Hours 1-2)

Thorough documentation is critical for recovery, legal requirements, and learning. Document in real time—memories fade quickly.

Core Documentation Checklist

[ ] What happened - Detailed description of the incident

[ ] When you discovered it - Exact date and time

[ ] What systems/data are affected - Complete list

[ ] Who has been notified - Names, times, methods of contact

[ ] What immediate actions you took - Step-by-step log

[ ] Screenshots taken (if safe to do so)

Evidence Collection Checklist

[ ] Full screenshots (not crops) with visible URLs and timestamps

[ ] Email headers saved, not just message content

[ ] URLs and usernames of accounts involved

[ ] Dates/times of all incidents with time zones

[ ] Names of any witnesses

[ ] System logs exported and saved securely

[ ] Access logs reviewed and saved

Impact Documentation

For personal targeting incidents:

[ ] Document impact on work, sleep, mental health

[ ] Track missed work or reduced productivity

[ ] Medical visits or therapy sessions related to incident

[ ] Security measures taken (costs incurred)

Phase 3: Assess Scope (Hours 2-6)

Determine the full extent of the incident to guide response priorities and legal obligations.

System Security Assessment

[ ] Identify affected systems - What accounts/systems are compromised?

[ ] Review admin access - Check all administrative accounts

[ ] Audit recent changes - What was modified in the last 30 days?

[ ] Check backup integrity - Are backups clean and recent?

[ ] Review access logs - Who accessed what and when?

[ ] Scan for malware - Run security scans on affected systems

[ ] Update security software - Ensure all protections are current

Data Protection Assessment

[ ] What data was accessed? (Donor info, strategies, personal data)

[ ] What data was modified? (Check integrity of important files)

[ ] What data was exported? (Check for signs of data theft)

[ ] Who is affected? (Staff, donors, partners, community members)

[ ] How many people's data may be affected?

[ ] What types of data? (Contact info, financial, sensitive personal data)

[ ] What are legal obligations? (Breach notification requirements)

[ ] Insurance notification - Does cyber insurance need to know?

[ ] Whether the incident is contained or ongoing

Incident Prioritization Matrix

Use this matrix to determine response urgency:

HIGH PRIORITY (Address Immediately):

[ ] Public website defaced or down

[ ] Email systems compromised

[ ] Campaign operations disrupted

[ ] Staff unable to work safely

[ ] Donor systems affected

[ ] Donor payment information exposed

[ ] Social security numbers or personal ID info

[ ] Medical information of staff/community

[ ] Any information about minors

MEDIUM PRIORITY (Address Same Day):

[ ] Internal systems slow/unreliable

[ ] Non-critical services interrupted

[ ] Individual staff accounts compromised

[ ] Social media accounts affected

[ ] Internal campaign strategies leaked

[ ] Staff personal information exposed

[ ] Confidential partner communications

LOW PRIORITY (Address Within 48 Hours):

[ ] Minor harassment targeting individual

[ ] Attempted attacks that failed

[ ] Suspicious activity with no clear impact

[ ] General supporter lists

[ ] Public position papers or statements

Phase 4: Get Help (Hours 2-6)

Engage external expertise and coordinate with authorities as appropriate.

External Support Activation

[ ] Contact IT support/consultant

[ ] Notify cyber insurance carrier (if applicable)

[ ] Engage legal counsel for breach notification guidance

[ ] Contact coalition partners if they may be affected

[ ] Reach out for mental health support resources

Law Enforcement Coordination

Note: Whether to contact law enforcement should be determined by the Executive Director, given the current political climate. Consider the following:

Potential benefits of law enforcement involvement:

- Specialized cyber units have tools to help contain attacks
- Can assist in determining method of attack and data recovery
- Reporting may help with insurance claims
- May be required by state law for certain types of attacks

If contacting law enforcement:

[ ] Contact local police department (see emergency contacts)

[ ] Contact local FBI office for cyber incidents (see emergency contacts)

[ ] Coordinate with legal counsel on evidence handling

[ ] Continue coordination throughout recovery process

Team Coordination

[ ] Incident lead coordinates overall response

[ ] Technical responder handles systems/accounts

[ ] Communications lead manages messaging

[ ] Legal liaison coordinates with attorneys

[ ] Support coordinator manages staff wellbeing

[ ] Backup personnel identified for each role

Phase 5: Begin Recovery (Hours 6-24 and Beyond)

Restore operations and implement strengthened security measures.

System Recovery

[ ] Restore systems from clean backups

[ ] Verify backup integrity before restoration

[ ] Apply all security updates and patches

[ ] Review and strengthen access controls

[ ] Implement additional security measures based on incident

[ ] Test restored systems before bringing online

[ ] Monitor for continued threats

Legal Notifications

IMPORTANT: You may have legal obligations if data is stolen. Consult legal counsel immediately. When in doubt about notification requirements, err on the side of transparency.

You may need to notify authorities if:

[ ] 500+ individuals affected (notify state attorneys general)

[ ] Breach involves credit cards (notify card brands and banks)

[ ] Health information compromised (notify HHS within 72 hours)

[ ] Minors affected (additional state law requirements may apply)

You may need to notify individuals if:

[ ] Personal information likely to result in harm was accessed

[ ] Financial information was compromised

[ ] Social Security numbers were accessed

[ ] State law requires notification (varies by state)

Notification checklist:

[ ] Develop detailed incident timeline

[ ] Assess legal notification requirements with counsel

[ ] File required regulatory reports

[ ] Notify affected individuals as required

Stakeholder Communications

[ ] Plan stakeholder communications

[ ] Update Board of Directors

[ ] Brief all staff with password change instructions

[ ] Notify coalition partners as appropriate

[ ] Prepare holding statements for media if needed

[ ] Document all response actions taken

Phase 6: Learning and Improvement (Post-Incident)

Every incident is an opportunity to strengthen your security posture. Conduct a thorough review after the immediate crisis has passed.

Incident Review Process

[ ] Conduct incident review meeting with response team

[ ] Document what worked well in the response

[ ] Identify what could be improved

[ ] Review timeline of events and response actions

[ ] Assess whether all procedures were followed

[ ] Evaluate team coordination and communication

Security Improvements

[ ] Update security procedures based on lessons learned

[ ] Implement additional protective measures

[ ] Review and update access controls

[ ] Enhance monitoring and detection capabilities

[ ] Review backup procedures and test restoration

Training and Awareness

[ ] Provide additional staff training based on incident type

[ ] Share lessons learned with all staff (appropriately)

[ ] Update security awareness materials

[ ] Schedule regular security training refreshers

Plan Updates

[ ] Review and update incident response plan

[ ] Test updated procedures with tabletop exercises

[ ] Update contact lists and escalation procedures

[ ] Ensure all staff know where to find updated plan

[ ] Schedule annual plan review and update

BUSINESS CRITICAL ASSETS

Identify the systems, networks, and data that are essential to your organization's mission. Understanding what's critical helps you prioritize protection and response efforts.

Mission Critical Systems

These systems are responsible for executing functions your organization depends on to meet its stated goals. Failure of these systems may result in a complete inability to continue key operations.

Examples: Email system, donor database, website, advocacy platform

Your mission critical systems:

Business Critical Systems

These systems have specific functions in the effective delivery of your organization's service but are not responsible for overall operation. They often focus on management of assets. Failure would disrupt service but not shut down operations entirely.

Examples: HR system, accounting software, internal collaboration tools

Your business critical systems:

Safety Critical Systems

These systems are used to protect the physical safety of your organization's personnel and environment.

Examples: Building access control, surveillance systems, emergency notification system

Your safety critical systems:

Critical Data Assets

Identify your most sensitive and valuable data assets:

Incident Response Cheat Sheets: 5 Critical Steps for Digital Emergency Response

Follow these steps immediately when an incident occurs:

Step 1: STOP & DOCUMENT

- STOP using the affected account or device immediately
- Don't panic—take a breath and think clearly
- Take screenshots with full URLs and timestamps (not crops)
- Document what happened, when you noticed, what you clicked/saw
- Preserve evidence—don't delete anything, even if embarrassing
- Save email headers, not just message content

Why this matters: Your first action is to preserve evidence. Don't inadvertently delete information that can help you recover.

Step 2: ACTIVATE YOUR RESPONSE TEAM

Call contacts in this order (within 1 hour):

- 1. Incident Commander
- 2. Technical Lead
- 3. Communications Lead
- 4. Executive Contact

Template message: "*We have a security incident involving [brief description]. I've documented what happened. Need immediate coordination—switching to Signal for secure comms.*"

- **Switch to Signal or encrypted channels immediately**

Step 3: SECURE THE SCENE

Immediate containment actions:

- Change passwords for affected accounts from a clean device
- Enable 2FA on all accounts if not already active
- Disconnect compromised devices from network (unplug ethernet/turn off WiFi)
- Review recent account activity for unauthorized access
- Alert personal contacts about potential impersonation

What NOT to do:

- Don't restart or shut down compromised systems
- Don't delete suspicious files or emails
- Don't communicate about the incident over potentially compromised channels

Step 4: ASSESS THE SCOPE

Key questions to answer:

- What data was accessed or compromised? (donor info, strategies, personal data)
- How many people's data may be affected?
- What types of data? (contact info, financial, sensitive personal data)
- Is the incident contained or ongoing?
- Can we fix it ourselves or do we need external help?
- Are other organizations or coalition partners affected?

Step 5: BEGIN RECOVERY

- Restore systems from clean backups
- Apply security updates and patches
- Review and strengthen access controls
- Monitor for continued threats
- Notify affected individuals if required by law
- File required regulatory reports
- Update Board and stakeholders as appropriate

ANNEX: COMMON INCIDENT TYPES

This plan applies to incidents including:

- **Doxxing attacks** - Personal information published online
- **Account compromises** - Unauthorized access to email, social media, or organizational accounts
- **Phishing attacks** - Malicious emails targeting staff
- **Harassment campaigns** - Coordinated online abuse or intimidation
- **Data breaches** - Donor information, strategies, or sensitive documents exposed
- **Website attacks** - Site hacked, defaced, or taken offline
- **Ransomware** - Digital assets frozen by an attacker
- **Surveillance detection** - Discovering monitoring at events or through digital means
- **Impersonation** - Fake accounts or profiles pretending to be you/your organization
- **Legal threats** - SLAPP suits, subpoenas, or aggressive legal demands
- **Physical security concerns** - Threats crossing from digital to real-world safety

Document Version Control

Record all updates to this plan below:

Date	**Updated By**	**Changes Made**