

Organizational Incident Response Checklist

Incident Response Checklist (First 30 Minutes)

Immediate Actions

- ☐ **STOP** - Don't continue using compromised accounts/systems
- ☐ **Document everything** - Screenshot with timestamps before systems change
- ☐ **Assess safety** - Is there immediate physical threat to staff?
- ☐ **Alert incident lead** - Contact primary incident responder immediately
- ☐ **Preserve evidence** - Don't delete anything, even if embarrassing
- ☐ **Activate secure communications** - Switch to Signal/encrypted channels
- ☐ **Brief assessment** - What type of incident appears to be occurring?

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

Organizational Security Incident Checklist

Team Activation

- ☐ **Incident lead** takes charge of coordination
- ☐ **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

System Security Assessment

- ☐ **Identify affected systems** - What accounts/systems are compromised?
- ☐ **Change compromised passwords** immediately
- ☐ **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?
- ☐ **What are legal obligations?** - Breach notification requirements?
- ☐ **Insurance notification** - Does cyber insurance need to know?

Incident Prioritization Matrix

Functional Impact Assessment

High Priority (Address Immediately):

- ☐ Public website defaced or down
- ☐ Email systems compromised

- ☐ Campaign operations disrupted
- ☐ Staff unable to work safely
- ☐ Donor systems affected

Medium Priority (Address Same Day):

- ☐ Internal systems slow/unreliable
- ☐ Non-critical services interrupted
- ☐ Individual staff accounts compromised
- ☐ Social media accounts affected

Low Priority (Address Within 48 Hours):

- ☐ Minor harassment targeting individual
- ☐ Attempted attacks that failed
- ☐ Suspicious activity with no clear impact

Information Impact Assessment

Critical (Legal/Regulatory Requirements):

- ☐ Donor payment information exposed
- ☐ Social security numbers or personal ID info
- ☐ Medical information of staff/community
- ☐ Any information about minors

High Sensitivity:

- ☐ Internal campaign strategies leaked
- ☐ Staff personal information exposed
- ☐ Confidential partner communications
- ☐ Opposition research or sensitive plans

Medium Sensitivity:

- ☐ General supporter lists
- ☐ Public position papers or statements
- ☐ Organizational financial information

- ☐ Non-sensitive staff communications

Communication Protocol Checklists

Internal Communications

- ☐ **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 scheduled** - frequency depends on severity
- ☐ **Roles clarified** - who's handling what aspects
- ☐ **Work modifications** - what should staff stop/start doing?
- ☐ **Mental health support** offered to affected staff

External Communications Decision Tree

DO NOT contact external parties until you've answered:

- ☐ Do we understand what happened?
- ☐ Have we stopped the immediate problem?
- ☐ Do we have legal advice if needed?
- ☐ What is our key message?

Media Inquiries:

- ☐ Refer to designated spokesperson only
- ☐ Use pre-approved holding statements
- ☐ Don't speculate about cause or scope
- ☐ Focus on what you're doing to address it
- ☐ Emphasize commitment to security and transparency

Partner/Coalition Notifications:

- ☐ Alert partners if they might be affected
- ☐ Share technical indicators (IPs, domains) if relevant
- ☐ Coordinate messaging if it's a sector-wide issue

- ☐ Request additional resources if needed

Law Enforcement Contact:

- ☐ Consult legal counsel first
- ☐ Prepare incident timeline and evidence
- ☐ Designate single point of contact
- ☐ Understand what you're asking for (investigation vs. advice)

Evidence Preservation Checklist

Digital Evidence

- ☐ **Screenshots with timestamps** of all relevant activity
- ☐ **Full email headers** saved, not just message content
- ☐ **Browser history** exported before clearing
- ☐ **Log files** copied to secure storage
- ☐ **Account activity reports** downloaded
- ☐ **Social media posts** archived with metadata
- ☐ **File system snapshots** of affected computers

Chain of Custody Documentation

For each piece of evidence:

- ☐ **What** - Specific description of evidence
- ☐ **When** - Date and time collected (with time zone)
- ☐ **Who** - Name and role of person collecting
- ☐ **Where** - Location/system evidence came from
- ☐ **Why** - Relevance to the incident
- ☐ **How** - Method used to collect/preserve
- ☐ **Chain** - Who has handled it since collection

Recovery and Lessons Learned Checklists

System Recovery

- ☐ **Malware removed** from all affected systems
- ☐ **Vulnerabilities patched** that were exploited
- ☐ **Passwords changed** on all potentially affected accounts
- ☐ **Access controls reviewed** and updated
- ☐ **Backup systems tested** and verified clean
- ☐ **Monitoring enhanced** for ongoing threats
- ☐ **Security software updated** across all systems
- ☐ **Normal operations restored** and tested

Post-Incident Review (Within 1 Week)

- ☐ **Timeline documented** - What happened when?
- ☐ **Response effectiveness evaluated** - What worked/didn't work?
- ☐ **Root cause identified** - How did this happen?
- ☐ **Lessons learned captured** - What would we do differently?
- ☐ **Process improvements identified** - What needs to change?
- ☐ **Training needs assessed** - Who needs additional training?
- ☐ **Policy updates required** - What policies need revision?
- ☐ **Follow-up actions assigned** - Who does what by when?

Prevention Improvements

- ☐ **Security awareness training** updated with lessons learned
- ☐ **Technical controls enhanced** based on attack vector
- ☐ **Monitoring improved** to detect similar attacks faster
- ☐ **Response procedures updated** based on what we learned
- ☐ **Vendor security reviewed** if third-party systems involved
- ☐ **Insurance claims filed** if applicable

- ☐ **Regulatory notifications completed** if required

Quick Reference: When to Escalate

Immediate Escalation Required

- ☐ Any threat of physical violence
- ☐ Suspected criminal activity (hacking, stalking, threats)
- ☐ Social security numbers or payment card data compromised
- ☐ Systems completely down/inaccessible
- ☐ Coordinated attack affecting multiple organizations
- ☐ Media already reporting on the incident

Escalate Within 24 Hours

- ☐ Email systems compromised
- ☐ Donor information potentially accessed
- ☐ Website defaced or hijacked
- ☐ Staff personal information exposed
- ☐ Suspected state-sponsored or sophisticated attack
- ☐ Attack methods unknown to your technical team

Monitor and Address Internally

- ☐ Individual staff member receiving harassment
- ☐ Password spray attacks that were blocked
- ☐ Phishing attempts caught by filters
- ☐ Minor social media account compromise
- ☐ Suspicious but unsuccessful login attempts

Emergency Contacts Template

Keep this information readily accessible and secure:

Primary Incident Response Team

- **Incident Lead:** _____ (Phone: _____, Signal: _____)
- **Technical Lead:** _____ (Phone: _____, Signal: _____)
- **Communications Lead:** _____ (Phone: _____, Signal: _____)
- **Executive Contact:** _____ (Phone: _____, Signal: _____)

External Support

- **Legal Counsel:** _____ (Phone: _____, Available: _____)
- **Technical Support:** _____ (Phone: _____, Signal: _____)
- **Mental Health Support:** _____ (Phone: _____, Crisis Line: _____)
- **Coalition Partners:** _____ (Phone: _____, Signal: _____)

Emergency Services

- **Local Law Enforcement:** _____ (Phone: _____)
- **FBI Field Office:** _____ (Phone: _____)
- **State Attorney General:** _____ (Phone: _____)
- **Crisis Counseling:** _____ (Phone: _____)

Key Account Recovery Information

- **Domain Registrar:** _____ (Account: _____, Phone: _____)
 - **Web Hosting:** _____ (Account: _____, Phone: _____)
 - **Email Provider:** _____ (Admin: _____, Phone: _____)
 - **Social Media:** _____ (Account: _____, Recovery: _____) *Remember: Print and store this securely. Review and update every 6 months. Practice using these checklists during tabletop exercises.*
-