Incident Response Plan

Table of Contents

[Purpose and Scope 1](#_Toc202959835)

[Incident Response Team and Roles 1](#_Toc202959836)

[Core Team Structure 1](#_Toc202959837)

[External Support Team 2](#_Toc202959838)

[Incident Classification and Severity 2](#_Toc202959839)

[Incident Types 3](#_Toc202959840)

[Severity Levels 3](#_Toc202959841)

[Response Phase Checklists 4](#_Toc202959842)

[Phase 1: Detection and Initial Assessment 4](#_Toc202959843)

[Evidence Preservation Guidelines 5](#_Toc202959844)

[Phase 2: Third-Party Support Activation 6](#_Toc202959845)

[Phase 3: Investigation and Containment 7](#_Toc202959846)

[Phase 4: Eradication and Recovery 8](#_Toc202959847)

[Phase 5: Return to Operations (Variable timing) 9](#_Toc202959848)

[Scenario-Specific Guidelines 9](#_Toc202959849)

[Ransomware/Malware Incidents 9](#_Toc202959850)

[Suspicious System Activity Incidents 10](#_Toc202959851)

[Data Disclosure/Spillage Incidents 11](#_Toc202959852)

[System Compromise Incidents 12](#_Toc202959853)

[Vendor/Third-Party Incidents 12](#_Toc202959854)

[Notification and Compliance Requirements 12](#_Toc202959855)

[Data Breach Communication Guidelines 13](#_Toc202959856)

[Mandatory North Dakota Notifications 13](#_Toc202959857)

[Federal Notification Requirements 14](#_Toc202959858)

[Other Required Notifications 14](#_Toc202959859)

[Data Incident vs. Data Breach Determination 15](#_Toc202959860)

[Terminology Guidelines 15](#_Toc202959861)

[Decision Framework 15](#_Toc202959862)

[Credit Monitoring and Identity Protection 16](#_Toc202959863)

[Technical Support Coordination 16](#_Toc202959864)

[Service Level Agreement (SLA) Considerations 17](#_Toc202959865)

[Recovery and Lessons Learned 18](#_Toc202959866)

[Recovery Verification 18](#_Toc202959867)

[After-Action Review Process 18](#_Toc202959868)

[Plan Maintenance and Testing 19](#_Toc202959869)

[Annual Plan Review 19](#_Toc202959870)

[Testing and Exercises 19](#_Toc202959871)

[Continuous Improvement and Plan Updates 19](#_Toc202959872)

[Revision History 20](#_Toc202959873)

[APPENDIX A: Contact Information 21](#_Toc202959874)

[Internal Emergency Contacts 21](#_Toc202959875)

[External Support Contacts 21](#_Toc202959876)

[Regulatory and Law Enforcement 21](#_Toc202959877)

[APPENDIX B: ND Cybersecurity and Data Breach Reporting Requirements 22](#_Toc202959878)

[NDIT Cybersecurity Incident Reporting *(NDCC 54-59.1)* 22](#_Toc202959879)

[ND Attorney General Data Breach Notification *(NDCC 51-30)* 23](#_Toc202959880)

[APPENDIX C: Severity Assessment Worksheet 24](#_Toc202959881)

How to Use this Plan



# Purpose and Scope

Purpose

This Cybersecurity Incident Response Plan provides a structured approach for detecting, responding to, containing, and recovering from cybersecurity incidents. It is designed for organizations with limited internal IT resources who rely primarily on third-party support providers, including managed service providers (MSPs) and the North Dakota Information Technology Department (NDIT).

This plan coordinates with the organization’s Crisis Management & Communications Plan and Business Continuity Plan to provide comprehensive response.

Scope

This plan applies to all technology systems, data, and operations within the organization, encompassing both physical and digital assets that could be affected by cybersecurity incidents.

**For K-12 Schools:** The plan covers all school technology systems and data, including student information systems, educational technology platforms, administrative systems, and staff and student devices.

**For Cities and Counties:** The plan covers all municipal technology systems and data, including public service delivery systems, financial and administrative systems, citizen-facing services and websites, and public safety systems with coordination to emergency management protocols.

This plan applies to:

Key Assumptions

This plan assumes organizations use NDIT network services and rely primarily on third-party vendors for technical support. Most organizations covered by this plan have limited internal cybersecurity expertise and need guidance for rapid vendor coordination and regulatory compliance.

# Incident Response Team and Roles

## Core Team Structure

**Incident Response Coordinator** (*K-12:* Superintendent or Principal | *Cities/Counties:* Mayor, City Manager, or Department Head)

* Activates incident response plan
* Makes critical decisions about operations
* Authorizes external communications
* Approves resource allocation

**IT Coordinator** *(K-12:* Technology Director/Coordinator | *Cities/Counties:* IT Manager or designated staff)

* Leads technical response coordination
* Primary contact with IT support vendors
* Coordinates with NDIT
* Documents technical aspects

**Communications Coordinator** (*K-12:* Administrative Assistant or designated staff | *Cities/Counties:* Communications Director or designated staff)

* Manages stakeholder notifications
* Coordinates with Crisis Communication Plan
* Handles media inquiries per established protocols

**Data/Privacy Officer** (*K-12: Registrar, Administrative Assistant, or Principal | Cities/Counties:* Clerk, Administrator, or designated staff)

* Assesses data exposure
* Determines notification requirements
* Coordinates affected individual notifications

## External Support Team

**Primary IT Support Vendor/MSP**

* Technical incident response leadership
* System restoration and security
* Evidence preservation and analysis

**NDIT (North Dakota Information Technology)**

* Network-level support and monitoring
* State-level incident coordination
* Regulatory compliance assistance

**Legal Counsel** (as needed)

* Regulatory compliance guidance
* Liability and risk assessment
* Media and legal strategy

**Cyber Insurance Provider** (if applicable)

* Claims process management
* Coverage verification
* Additional resource provision

# Incident Classification and Severity

Proper incident classification helps organizations allocate appropriate resources and determine the urgency of response actions. This section defines the types of cybersecurity incidents organizations may encounter and establishes four severity levels to guide response efforts. Use the Severity Assessment Worksheet in [Appendix C](#_APPENDIX_C:_Severity) to systematically evaluate incidents and document severity determinations throughout the response process.

## Incident Types

Malware/Ransomware. These incidents involve malicious software affecting systems, including file encryption or system lockout, and performance degradation from malware infections.

Suspicious System Activity. This category covers unusual system behavior or performance issues, unexpected access attempts or account activity, suspicious network connections or data transfers, and signs of potential compromise requiring investigation.

Data Disclosure/Spillage. These incidents involve potential unauthorized access to sensitive data, accidental exposure of confidential information, or suspected data theft or inappropriate access. Note that "data incident" language should be used until confirmed as a breach.

System Compromise. This type includes confirmed unauthorized access to systems, account takeovers or privilege escalation, and evidence of malicious control or manipulation.

Vendor/Third-Party Incidents. These involve security incidents at service providers, cloud service disruptions, or supply chain compromises.

Network/Infrastructure Issues. This category covers network outages or disruptions, DDoS attacks, and infrastructure failures.

## Severity Levels

Level 1 - Low Impact

* Single system or limited user impact
* No sensitive data involved
* Minimal operational disruption
* *Response:* Standard IT support procedures
* *Timeline:* Resolve within 4-8 hours

Level 2 - Medium Impact

* Multiple systems affected
* Possible limited data disclosure
* Noticeable operational impact
* *Response:* IT Coordinator + vendor support
* *Timeline:* Resolve within 24-48 hours

Level 3 - High Impact

* Critical systems affected
* Confirmed data disclosure or major system compromise
* Significant operational disruption
* *Response:* Full incident response team activation
* *Timeline:* Resolve within 48-72 hours

Level 4 - Critical Impact

* Major systems completely compromised
* Extensive data disclosure or complete system failure
* Operations severely impacted or halted
* *Response:* All resources, emergency procedures
* *Timeline:* Extended recovery period

# Response Phase Checklists

The incident response process follows five distinct phases, each with specific objectives and actions. These phases provide a structured approach to managing cybersecurity incidents from initial detection through full recovery. While the phases are presented sequentially, some activities may overlap, and organizations may need to cycle back to earlier phases as new information emerges. The checklists in each phase are designed to be actionable during high-stress situations and can be adapted based on available resources and the specific nature of the incident.

## Phase 1: Detection and Initial Assessment

This initial phase focuses on quickly understanding what has occurred and taking immediate protective steps to prevent further damage. The priority is gathering essential facts, preserving evidence, and implementing basic containment measures. Any staff member may detect and report an incident, but the IT Coordinator takes leadership for technical assessment while the Incident Response Coordinator makes decisions about plan activation and resource allocation.

**Initial Detection**

Document the incident

* Time of discovery
* Who reported it
* Initial symptoms observed
* Systems or data potentially affected

Preserve evidence

* Take screenshots of error messages
* Do NOT power off affected systems
* Document any unusual network activity
* Save any suspicious files or emails

Immediate safety assessment

* Are any systems actively being compromised?
* Is data currently being accessed or stolen?
* Are other systems at immediate risk?

Notify IT Coordinator

* Provide initial assessment
* Share documentation collected
* Determine severity level

**Initial Containment (if safe to do so)**

Isolate affected systems (only if you can do so safely)

* Preferred method: Use security tools (XDR, endpoint protection) to quarantine devices

Alternative method: Disconnect from network (unplug network cable) only if security tools are unavailable

* Do NOT: Shut down computers (may lose evidence)
* Do NOT: Physically remove devices until consulting with IT support vendor
* Block suspicious IP addresses if known and possible
* Disable compromised user accounts

Alert key personnel

* Incident Response Coordinator
* Communications Coordinator (for potential notifications)
* Department heads of affected areas

## Evidence Preservation Guidelines

Before ANY Technical Intervention

Proper evidence preservation is critical for potential legal proceedings, insurance claims, and forensic analysis. Before any technical work begins, document the current system state with screenshots, record exact error messages and timestamps, and note what users were doing when the incident occurred. Take photographs of any ransom notes or unusual displays, export current system logs if safely accessible, and document network connections and suspicious IP addresses.

During Technical Response Coordination

When working with technical support resources, inform the technical lead of evidence preservation needs before they begin work. Request documentation of all investigative steps and ask for forensic images to be created before cleanup if the capability exists. Establish clear evidence handoff procedures, maintain chain of custody documentation, and get agreement on evidence preservation timelines.

Key Technical Response Discussions:

* "We need to preserve evidence for potential law enforcement/insurance"
* "Please document your analysis before making any changes"
* "Can forensic copies be created before starting remediation?"
* "What evidence will be destroyed by the cleanup process?"

Never Allow Technical Response Team To:

* Start cleanup without documenting current state
* Delete files without explicit approval from Incident Response Coordinator
* Restore from backups before evidence collection
* Make system changes without logging what was done

Documentation Requirements:

* Time-stamped log of all technical actions
* Screenshots/photos before and after technical work
* Written summary of technical findings
* Copies of any analysis reports
* Record of what evidence was preserved vs. destroyed during recovery

## Phase 2: Third-Party Support Activation

Once the incident scope is understood, this phase mobilizes the external resources needed for technical response and regulatory compliance. The Incident Response Coordinator authorizes vendor engagement and associated costs, while the IT Coordinator manages technical access and coordinates with support providers. Early coordination with insurance and regulatory authorities in this phase can significantly impact response effectiveness and legal compliance.

**Vendor Coordination**

Contact Primary IT Support Vendor/MSP

* Report incident type and severity
* Provide access to affected systems
* Request immediate response time estimate
* Confirm escalation procedures

Notify NDIT (Required for all cybersecurity incidents)

* Contact: NDIT Service Desk at 701-328-4470
* Report to: <https://www.ndit.nd.gov/support/report-cyber-security-incident>
* Provide: Organization name, incident type, affected systems
* Request: Technical assistance if needed

Activate cyber insurance (if applicable)

* Contact insurance provider
* Report incident details
* Verify coverage for response costs
* Request claim number

**Information Gathering**

Collect baseline information

* Network diagrams and system inventory
* Recent backup information
* User account lists
* Recent system changes or updates

Establish communication channels

* Set up dedicated incident response communication (phone, secure email)
* Create shared documentation space
* Establish regular update schedule with vendors

**Activate Crisis Communications (if needed)**

* Consult Crisis Management & Communication Plan for notification triggers
* Notify Communications Coordinator if incident may require public communication
* Refer to Crisis Communication Plan for stakeholder notification procedures
* Document when/why crisis communications were activated

## Phase 3: Investigation and Containment

This phase combines detailed technical investigation with enhanced protective measures to fully understand the incident scope and prevent further compromise. The technical lead (IT Coordinator or designated expert) approves specific containment measures and investigative approaches, while the Incident Response Coordinator authorizes broader security controls and operational changes. The Data/Privacy Officer takes responsibility for data exposure assessments that will drive notification requirements.

**Technical Investigation (Led by available technical resources)**

Support technical analysis

* Internal IT Staff: Provide access to affected systems and assist with evidence collection
* Third-Party Support: Coordinate access and share system information as needed
* Vendor Systems: Work with vendor technical teams following their incident procedures
* NDIT Support: Coordinate with state resources if assistance is needed

Assess scope and impact

* Identify all affected systems with available technical resources
* Determine potential data exposure using system logs and access records
* Estimate number of affected users/records
* Document timeline of incident
* **Important:** Use "data incident" language until confirmed as breach

Technical Resource Coordination

* Document who I s leading technical response
* Establish clear communication channels with technical lead
* Define roles and responsibilities for evidence collection
* Set expectations for technical reporting and updates

**Enhanced Containment**

Implement additional security measures

* Change administrative passwords
* Disable unnecessary user accounts
* Apply emergency patches or configurations
* Increase monitoring on critical systems

Protect unaffected systems

* Verify backup system integrity
* Implement additional access controls
* Monitor for signs of spreading
* Secure critical data repositories

## Phase 4: Eradication and Recovery

With the threat understood and contained, this phase focuses on completely removing the threat and safely restoring normal operations. The technical lead confirms that threats have been fully eradicated before system restoration begins, the IT Coordinator approves the specific recovery approach and system restoration sequence, and the Incident Response Coordinator authorizes the transition from response to recovery operations.

**Business Continuity Assessment**

* Determine if alternate operations procedures are needed (see Business Continuity Plan)
* Assess whether extended outage triggers disaster recovery procedures
* Coordinate with Business Continuity Plan if normal operations cannot resume within [X hours]

**System Cleanup (Vendor-Led)**

Remove threats (using available technical capabilities)

* Clean malware from affected systems
* Close unauthorized access points
* Remove malicious files or code
* Verify complete threat removal

Patch vulnerabilities

* Apply security updates within technical capabilities
* Fix configuration weaknesses
* Strengthen access controls
* Update security software

Technical Capability Assessment

* Document what can be done with internal resources
* Identify when external technical assistance is needed
* Coordinate between internal staff and external support
* Escalate to specialized resources when needed (forensics, advanced malware analysis, etc.)

**Recovery Planning**

Prioritize system restoration

* Critical operational systems first
* Essential data and applications
* User access and productivity tools
* Secondary and convenience systems

Validate system integrity

* Test systems in an isolated environment
* Verify data integrity and completeness
* Confirm security controls are working
* Document changes made during recovery

## Phase 5: Return to Operations (Variable timing)

**Phased Restoration**

Gradual system return

* Return critical systems to production
* Monitor for any signs of issues
* Gradually restore user access
* Verify normal operations

Enhanced monitoring

* Implement additional logging
* Increase security monitoring
* Watch for signs of reinfection
* Document successful restoration

**User Communication**

Prepare users for return

* Notify about system availability
* Provide any new procedures
* Share security reminders
* Establish support channels for issues

# Scenario-Specific Guidelines

While the five-phase response process provides a consistent framework for all incidents, different types of cybersecurity incidents may require specialized considerations and approaches. This section provides additional guidance for common incident scenarios that organizations are likely to encounter. These guidelines supplement the standard response phases and highlight critical decision points, unique considerations, and scenario-specific actions that may be necessary. Organizations should use these guidelines in conjunction with the phase-based checklists to ensure comprehensive incident response tailored to the specific nature of each event.

## Ransomware/Malware Incidents

**Immediate Actions**

Isolation Protocol

* Immediately isolate affected systems from network
* Do NOT power off systems (preserve memory evidence)
* Take photos of ransom messages or unusual screens
* Document affected file types and locations

Ransom Assessment

* Document ransom amount and payment instructions
* Do NOT contact attackers without legal consultation
* Evaluate backup availability and integrity
* Assess operational impact of extended downtime

**Decision Framework**

Backup Evaluation

* Verify backup systems are unaffected
* Test restore capability from recent backups
* Identify any gaps in backup coverage
* Estimate recovery time from backups

Ransom Payment Consideration (Legal/Leadership Decision)

* Consult with legal counsel and cyber insurance
* Consider law enforcement guidance
* Evaluate business continuity needs
* Document decision-making process

## Suspicious System Activity Incidents

**Initial Response**

Document Observations

* Record specific unusual behaviors (slow performance, unexpected pop-ups, etc.)
* Note any suspicious network activity or connections
* Document unusual user account activity
* Take screenshots of any error messages or suspicious screens

Preserve Evidence

* Do NOT immediately change passwords (may alert attackers)
* Keep affected systems running for analysis
* Monitor for additional suspicious activity
* Document timeline of observed behaviors

**Investigation Support**

Gather Investigation Data

* Collect system logs and network traffic data
* Review recent user access logs
* Check for unauthorized software installations
* Document any recent system or security changes

Determine Attack Vector (During vendor investigation)

* Email-based attacks (phishing, malicious attachments)
* Social engineering attempts
* Direct system exploitation
* Stolen or compromised credentials

## Data Disclosure/Spillage Incidents

**Immediate Assessment**

Data Incident Evaluation

* Identify types of data potentially accessed or disclosed
* Estimate number of affected individuals
* Determine sensitivity level of disclosed data
* Document evidence of data access vs. potential access only

Incident vs. Breach Determination

* Data Incident: Potential or suspected unauthorized access
* Data Breach: Confirmed unauthorized acquisition compromising security/confidentiality
* Consult with legal counsel before using "breach" terminology
* Document decision-making process for classification

**Regulatory Assessment**

North Dakota Breach Trigger Evaluation

* Does incident affect more than 250 North Dakota residents?
* What types of personal information involved?
* Has security, confidentiality, or integrity been compromised?
* Timeline requirements for formal breach notifications

Federal Requirements (if applicable)

* **K-12:** FERPA considerations for student educational records
* **Cities/Counties:** Other federal regulations based on data types
* Document regulatory applicability assessment

**Evidence Documentation**

Preserve All Evidence

* System logs showing unauthorized access attempts
* Evidence of actual data extraction or viewing
* Timeline of unauthorized activities
* Methods used to gain access to data
* Documentation of what data was actually accessed vs. potentially accessible

## System Compromise Incidents

**Access Control Review**

Account Security

* Identify compromised user accounts
* Force password resets for affected accounts
* Review administrative account access
* Audit recent account changes or additions

Privilege Escalation Check

* Review administrative actions taken
* Check for unauthorized system changes
* Verify integrity of security controls
* Document any unauthorized access or modifications

## Vendor/Third-Party Incidents

**Vendor Coordination**

Information Gathering

* Contact vendor for incident details
* Determine data and services affected
* Request vendor's incident response timeline
* Understand potential impact on your operations

Service Continuity

* Identify alternative service options
* Implement workaround procedures
* Communicate service disruptions to users
* Plan for extended vendor service outage

# Notification and Compliance Requirements

Cybersecurity incidents often trigger various legal, regulatory, and contractual notification obligations that must be fulfilled within specific timeframes. Understanding these requirements and acting promptly is essential for regulatory compliance and can significantly impact the organization's legal exposure and relationships with stakeholders. This section outlines the mandatory notifications required under North Dakota law, federal requirements that may apply, and other critical notifications to insurance providers and affected individuals. Organizations should consult with legal counsel when determining notification requirements, especially for incidents involving potential data exposure.

**NOTE:** For detailed communication procedures and message templates, see Crisis Management & Communication Plan. This section focuses on regulatory/legal notifications only.

## Data Breach Communication Guidelines

Proper terminology is critical when communicating about potential data exposure incidents. Using incorrect language can create unnecessary legal obligations or fail to provide adequate protection when obligations do exist. Organizations should distinguish between suspected data incidents under investigation and confirmed data breaches that trigger formal notification requirements.

Internal Communications:

* Use "data security incident" or "data disclosure incident" initially
* Avoid "breach" terminology until legal determination is made
* Focus on response actions and protective measures
* Document when language escalates to "breach" designation

External Communications:

* Coordinate with legal counsel on public-facing language
* Ensure consistency across all communication channels
* Consider stakeholder impact of terminology choices
* Reserve "breach" announcements for confirmed legal breaches

## Mandatory North Dakota Notifications

**NDIT Notification (Required for ALL cybersecurity incidents)**

Immediate Notification

* Contact: NDIT Service Desk at 701-328-4470
* Online: <https://www.ndit.nd.gov/support/report-cyber-security-incident>
* Timeframe: As soon as possible after discovery
* Information Required:
  + Organization name and contact information
  + Incident type and description
  + Affected systems and potential data
  + Current status and response actions
  + Assistance needed

**North Dakota Attorney General Notification (Data breaches affecting >250 individuals)**

Legal Notification Requirements

* Contact: ND Consumer Protection Division
* Timeframe: Most expedient time possible without unreasonable delay
* Triggers: Confirmed breach affecting 250 or more individuals. This threshold is total individuals affected, but notification applies when ND residents are among those affected.
* Important: This applies only to confirmed breaches, not data incidents under investigation.
* Information Required:
  + Description of the confirmed breach
  + Type of information compromised
  + Steps taken to protect affected individuals
  + Contact information for further details

## Federal Notification Requirements

**For K-12 Schools**

Department of Education (if student records affected)

* FERPA considerations for student educational records
* Privacy Technical Assistance Center guidance
* State education department notification if required

**For Cities/Counties**

Federal Agencies (if applicable)

* FBI for significant cyber incidents
* CISA for critical infrastructure impacts
* Department of Justice for criminal activity

## Other Required Notifications

**Cyber Insurance Provider**

Insurance Claim Process

* Timeframe: Immediately upon discovery (usually within 24-48 hours)
* Information Required:
  + Policy number and contact information
  + Detailed incident description
  + Estimated impact and damages
  + Response actions taken
* Follow-up: Provide regular updates and documentation

**Affected Individuals**

Individual Notification Requirements

* K-12: Parents/guardians and staff as appropriate
* Cities/Counties: Citizens and employees as appropriate
* Timeframe: Varies by incident type and state law
* Method: Written notice (email, mail) unless law enforcement requests delay
* Language Considerations: Use "data security incident" for potential exposures, "data breach" only for confirmed breaches
* Content Requirements:
  + Description of incident (avoid "breach" unless confirmed)
  + Types of information involved
  + Steps being taken to investigate
  + Steps individuals should take
  + Contact information for questions

# Data Incident vs. Data Breach Determination

One of the most critical decisions during a cybersecurity incident is determining whether a data exposure constitutes a legal "data breach" requiring formal notifications or remains a "data incident" under investigation. This determination has significant legal, regulatory, and communication implications. Making this classification too early can trigger unnecessary legal obligations, while delaying too long can result in non-compliance with notification requirements. Organizations should approach this determination systematically and with appropriate legal consultation.

## Terminology Guidelines

Data Security Incident (Initial response phase)

* Use for suspected or potential unauthorized access
* Appropriate when investigation is ongoing
* Allows for protective response without legal implications
* Can be escalated to "breach" if confirmed

Data Breach (Confirmed legal designation)

* Use only when unauthorized acquisition is confirmed
* Triggers formal legal notification requirements
* Requires legal counsel consultation
* Has specific regulatory and compliance implications

## Decision Framework

Several factors must be evaluated when determining breach classification:

* Unauthorized Acquisition: Was data actually accessed/stolen vs. potentially accessible?
* Security Compromise: Was the security, confidentiality, or integrity actually compromised?
* Legal Consultation: Has legal counsel confirmed breach designation?
* Regulatory Triggers: Do confirmed facts meet regulatory breach definitions?

Documentation Requirements

* Document decision-making process for incident classification
* Record factors considered in breach vs. incident determination
* Maintain timeline of when language escalated
* Keep legal consultation records for classification decisions

## Credit Monitoring and Identity Protection

When a cybersecurity incident involves exposure of personal information that could lead to identity theft, organizations may need to provide credit monitoring and identity protection services to affected individuals. This decision should be based on the types of information exposed, the number of people affected, and the potential for misuse. Offering these services demonstrates good faith effort to protect affected individuals and can help maintain trust and reduce liability exposure.

Assessment Criteria

Organizations should determine if credit monitoring is appropriate based on several factors. Consider whether Social Security Numbers were exposed, if financial account information was compromised, whether driver's license numbers or other identity information was involved, and evaluate the overall severity and scope of data exposure.

**Credit Monitoring Services**

Service Provider Selection:

* Free Options: Annual credit reports through annualcreditreport.com
* Paid Services: Commercial credit monitoring (Experian, Equifax, TransUnion)
* Duration: Typically, 1-2 years for significant breaches
* Coverage: May include credit monitoring, identity theft insurance, restoration services

Implementation Process:

* Vendor Procurement: Select and contract with monitoring service provider
* Communication: Provide clear instructions to affected individuals
* Enrollment: Assist individuals with service enrollment
* Duration: Monitor service effectiveness and renewal needs

Communication Coordination

Decisions about credit monitoring services should be communicated to affected individuals using the data breach notification templates and procedures outlined in the Crisis Management & Communication Plan. The Communications Coordinator should incorporate information about available identity protection services into the standard breach notification process.

# Technical Support Coordination

Most organizations rely on a combination of internal staff, third-party vendors, and external service providers for technical support during cybersecurity incidents. Coordinating these resources effectively is critical for successful incident response, especially when multiple technical teams may be working simultaneously on different aspects of the incident. This section provides guidance for activating and managing various technical support resources while maintaining clear communication channels and avoiding conflicts between different response teams.

## Emergency Technical Support Activation

Internal IT Resources

Organizations with internal IT staff should activate their emergency procedures and assign a lead technical coordinator. Document internal technical capabilities and limitations clearly and determine when external assistance is needed to supplement internal resources.

Third-Party IT Support (MSP/Consultant)

When engaging managed service providers or IT consultants, use established emergency contact procedures and provide the organization name, contact person, and brief incident description. Request immediate response time estimates and confirm escalation procedures, while verifying remote access availability and security protocols.

Vendor/Cloud Service Provider

For incidents involving specific vendor systems, follow the vendor's incident reporting procedures and request immediate technical assistance through their designated channels. Coordinate directly with vendor security teams and document their response actions and timelines.

NDIT Coordination

For network-level incidents affecting state systems, report the incident through official NDIT channels and request technical assistance for network-level issues. Coordinate response actions that may affect the state network and follow NDIT guidance for network protection measures.

Multi-Resource Coordination

When multiple technical resources are involved in an incident response, designate a single technical lead to avoid conflicts and ensure coordinated efforts. Establish clear communication protocols between all resources and define specific roles and responsibilities for each technical team or individual. Coordinate evidence preservation efforts across all technical teams to maintain proper chain of custody and documentation. Document all decisions about resource allocation and leadership to maintain clear accountability throughout the incident response process.

## Service Level Agreement (SLA) Considerations

When working with third-party vendors and managed service providers during incident response, understanding and managing service level agreements becomes critical for ensuring timely and effective technical support.

Response Time Expectations

Organizations should understand their vendor's response time commitments for different incident severities. Critical incidents typically require response within 1-2 hours, high priority incidents within 4 hours, and medium priority incidents within 8 hours. Document actual response times during incidents to ensure vendors are meeting their SLA commitments and identify any patterns of delayed response.

Escalation Procedures

Know when and how to escalate incidents with vendor management, including understanding escalation triggers and required timelines. Maintain backup vendor contacts for escalation purposes and document all escalation decisions and outcomes for future reference and vendor performance evaluation.

Vendor Communication Management

Establish regular status update schedules during incidents, typically hourly updates during critical phases. Request written status reports from vendors for proper documentation and ensure you understand their decision-making processes. Maintain your organization's oversight role throughout the incident response rather than simply deferring all decisions to the vendor.

Resource Coordination

Clarify how vendors will allocate resources to your incident and understand any additional cost implications for emergency or after-hours support. Coordinate vendor access to your facilities and staff as needed and manage vendor communications with your stakeholders to ensure consistent messaging and appropriate information sharing.

# Recovery and Lessons Learned

## Recovery Verification

System restoration is only the first step in returning to normal operations. Technical validation should confirm that all systems are restored and functioning normally, security patches and updates have been applied, threat removal has been verified through multiple methods, and backup systems are tested and operational. However, technical restoration must be accompanied by operational validation to ensure that critical business processes are verified, user access is restored and tested, essential functions work as expected, and stakeholders are confident in system integrity.

The Incident Response Coordinator holds ultimate authority for declaring that normal operations can resume, based on recommendations from the technical lead regarding system readiness and input from department heads about operational functionality. This decision should not be rushed, as premature return to operations can result in additional disruptions or security vulnerabilities.

## After-Action Review Process

Learning from incidents is essential for improving future response capabilities. An immediate debrief should be conducted within 48 hours of incident resolution, involving all key response personnel to review the timeline, evaluate vendor performance, assess decision-making processes, and identify immediate improvement opportunities. This initial review focuses on capturing fresh insights while the incident is still clear in everyone's memory.

A comprehensive review should follow within two weeks, providing time for more thorough analysis. This detailed assessment should examine all aspects of the response, analyze communication effectiveness throughout the incident, evaluate technology systems performance during the crisis, and identify specific policy and procedure improvements needed. The comprehensive review should result in concrete action items with assigned responsibilities and timelines.

# Plan Maintenance and Testing

## Annual Plan Review

This incident response plan should be reviewed annually to ensure it remains current and effective. During the annual review, update all contact information for both internal team members and external support providers, including verification of vendor emergency contact procedures and service level agreements. Review and update the technology inventory and system dependencies to reflect any changes in the organization's infrastructure. Ensure regulatory requirements haven't changed and that backup and recovery procedures remain valid. This is also an appropriate time to review staff roles and responsibilities and make any necessary adjustments based on organizational changes.

## Testing and Exercises

Regular testing helps ensure the plan will work effectively during an actual incident. Organizations should conduct tabletop exercises quarterly to walk through different incident scenarios and identify potential gaps or confusion in procedures. Communication systems should be tested monthly to verify that notification methods work properly and contact information is accurate. Contact lists should be verified quarterly to ensure all information remains current. A comprehensive review of the entire plan should be conducted annually, ideally incorporating lessons learned from any real incidents that occurred during the year.

## Continuous Improvement and Plan Updates

Incident response capabilities improve through systematic plan updates based on lessons learned from both real incidents and exercises. Document lessons learned from each exercise and any real incidents, then update procedures based on these findings. Track improvement actions to completion and share results with all incident response team members. When updating the plan, document all changes in the revision history table and ensure updated versions are distributed to all team members while removing outdated versions from circulation. Train staff on any significant procedural changes and coordinate updates with related plans such as Crisis Communication and Business Continuity to ensure consistency across all emergency response procedures.

# Revision History

| Date | Description | Changed by |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Document Control

* Version: 1.0
* Last Updated: [Date]
* Next Review Date: [Date + 1 year]
* Owner: [IT Coordinator Name]
* Approved by: [Incident Response Coordinator Name]

# APPENDIX A: Contact Information

## Internal Emergency Contacts

| Title/Function | Contact Name | Contact Information | Backup Resource |
| --- | --- | --- | --- |
| Incident Response Coord | Jane Smith | (e) [name@company.com](mailto:name@company.com)  (m) 111-222-3333  (h) 444-555-6666 | John McBackup |
| IT Coord |  |  |  |
| Communications Coord |  |  |  |
| Data/Privacy Officer |  |  |  |
|  |  |  |  |

## External Support Contacts

| Name / Function | Phone | Email/URL | Notes |
| --- | --- | --- | --- |
| ND Information Technology (NDIT) | 701-328-4470 | <https://www.ndit.nd.gov/support> |  |
| ND DES Watch Center |  | <https://www.des.nd.gov/response-section/webeoc> | This is optional and situationally based. |
| ND SLIC | 701-328-8172 |  |  |
| Legal Counsel |  |  |  |
| Cyber Insurance Provider |  |  |  |
|  |  |  |  |

## Regulatory and Law Enforcement

|  |  |  |
| --- | --- | --- |
| Entity | Contact Information | Reporting Requirements |
| ND Attorney General’s Office | (p) 701-328-3404  (e) [ndag@nd.gov](mailto:ndag@nd.gov) | Immediately for 250+ records as defined in [NDCC 51-30](https://www.ndlegis.gov/cencode/t51c30.pdf). |
| FBI | Internet Crime Complaint Center (IC3) <https://www.ic3.gov/> |  |
| ND Information Technology (NDIT) | <https://www.ndit.nd.gov/support/report-cyber-security-incident> | [NDCC 54-59.1](https://ndlegis.gov/cencode/t54c59-1.pdf#nameddest=54-59p1-01) |
|  |  |  |

# APPENDIX B: ND Cybersecurity and Data Breach Reporting Requirements

## NDIT Cybersecurity Incident Reporting *(*[*NDCC 54-59.1*](https://ndlegis.gov/cencode/t54c59-1.pdf#nameddest=54-59p1-01)*)*

Who Must Report: Executive branch agencies and political subdivisions

What Must Be Reported:

* Suspected data breaches involving government data
* Malware incidents with $10,000+ damage or mission capability loss
* Any cybersecurity concerns affecting confidentiality, integrity, or availability

How to Report:

* Phone: 701-328-4470 (NDIT Service Desk - 24/7)
* Online: <https://www.ndit.nd.gov/support/report-cyber-security-incident>
* When: As soon as possible after discovery

Required Information:

* Organization name and contact
* Incident date/time and description
* Affected systems and data
* Response actions taken
* Assistance needed

Follow-up: Provide updates on exposed records, affected individuals, and remediation efforts until resolved.

## ND Attorney General Data Breach Notification *(*[*NDCC 51-30*](https://ndlegis.gov/cencode/t54c59-1.pdf#nameddest=54-59p1-01)*)*

Who Must Report: Any entity with computerized personal information affecting 250 or more individuals (applies with ND residents are among those affected).

Personal Information Defined: Name + SSN, driver's license, financial account info, medical/health insurance info, or biometric data

Breach Defined: Unauthorized acquisition compromising security, confidentiality, or integrity of personal information

How to Report:

* Agency: Consumer Protection Division, ND Attorney General
* Phone: 701-328-3404
* Email: [consumerprotection@nd.gov](mailto:consumerprotection@nd.gov)
* When: Most expedient time possible without unreasonable delay

Required to Attorney General:

* Breach description
* Information types involved
* Number of ND residents affected
* Protection steps taken
* Contact info
* Copy of individual notices

Required to Individuals:

* Breach description
* Information involved
* Protection measures taken
* Steps individuals can take
* Contact info
* AG report notification

Exemptions: Good faith employee acquisition, encrypted data (key not compromised), low harm risk (documented)

# APPENDIX C: Severity Assessment Worksheet

|  |  |  |  |
| --- | --- | --- | --- |
| Completed By | Date | | Time |
|  |  | |  |
| How to Use This Assessment   * Read each impact level from top to bottom. * If you answer "YES" to ANY question in a level, that's your severity level. * Stop at the first level where you answer "yes" to any question. | | ❒ Initial Assessment  ❒ Reassessment | |

**ASSESSMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Question | | Yes | No | Unknown |
| **CRITICAL (Level 4)** | | | | |
|  | Are emergency services compromised? |  |  |  |
|  | Are safety systems affected |  |  |  |
|  | Is there immediate physical danger? |  |  |  |
|  | Are ALL critical systems down? |  |  |  |
| **HIGH (Level 3)** | | | | |
|  | Is one or more critical system completely down or inaccessible? |  |  |  |
|  | Are key operations severely impacted with limited workarounds? |  |  |  |
|  | Is there confirmed sensitive data exposure affecting 250+ people? |  |  |  |
|  | Are financial systems or payment processing compromised? |  |  |  |
|  | Will system recovery take more than 72 hours? |  |  |  |
| **MODERATE (Level 2)** | | | | |
|  | Are multiple systems affected but workarounds exist? |  |  |  |
|  | Is there suspected (but unconfirmed) data exposure? |  |  |  |
|  | Are administrative or support systems significantly impacted? |  |  |  |
|  | Will system recovery likely take 24-72 hours? |  |  |  |
|  | Will core operations be disrupted for 8-24 hours before alternate operating procedures can be implemented? |  |  |  |
|  | Is normal workflow significantly disrupted? |  |  |  |
|  | Are external communications or websites affected? |  |  |  |
| **LOW (Level 1)** | | | | |
|  | Is only a single system or limited users affected? |  |  |  |
|  | Are there minor performance issues or isolated incidents? |  |  |  |
|  | Can normal operations continue with minimal impact? |  |  |  |
|  | Will recovery likely take less than 24 hours? |  |  |  |
|  | Is this primarily a technical maintenance issue? |  |  |  |

**OUTCOME**

|  |  |
| --- | --- |
| Initial Severity | New Severity |
|  |  |
| Rationale / Reason for Change | |
| [Provide specific reasoning for the severity level or change in severity level.] | |

**KEY DETAILS**

|  |
| --- |
| Affected Systems/Services |
| [enter notes here] |
| Estimated Number of Users/Records Impacted |
| [enter notes here] |
| Suspected Cause (if known) |
| [enter notes here] |
| Other Relevant Factors |
| [enter notes here] |

**FOLLOW-UP ACTIONS**

* Notify Crisis Management Team
* Activate technical support
* Begin stakeholder communications
* Other

|  |  |
| --- | --- |
| Reassess severity when:   * New information about scope emerges * Recovery timelines change significantly * Data exposure extent becomes clearer * Additional systems become affected * Every 2 hours during active response | Always document:   * Initial severity assessment and rationale * Any severity level changes and why * Time of each reassessment |