SMALL BUSINESS INCIDENT RESPONSE POLICY

A practical guide for protecting your business technology assets.

Document Owner: [Your Name]
Effective Date: [Current Date]
Version 1.0

Contact Info:
Michael Nichols
manichols936@gmail.com
Connect/message me on LinkedIn

Disclaimer: This sample policy has been provided by Michael Nichols as a generic document to support the enhancement of your security posture. It is based on security frameworks, SOC 2 and NIST CSF, and has been adapted specifically for small business use. It is unlikely to be complete for your organization without customization. This document is not legal advice and I am independent of a registered CPA firm.

<table>
<tr><td colspan="8"><b>[Company Name]</b>
<b>Incident Response Policy</b></td></tr>
<tr><td colspan="2"><b>Effective Date:</b></td><td colspan="2"></td><td colspan="2"><b>Document Owner:</b></td><td colspan="2"></td></tr>
<tr><td colspan="8"><b>Revision History</b></td></tr>
<tr><td>Revision</td><td>Rev. Date</td><td>Description</td><td>Prepared By</td><td>Reviewed By</td><td>Date</td><td>Approved By</td><td>Date</td></tr>
<tr><td>1.0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

1. Purpose

This policy establishes clear guidelines for how our company responds to security incidents and data breaches. It defines what constitutes a breach, outlines staff

Disclaimer: This sample policy has been provided by Michael Nichols as a generic document to support the enhancement of your security posture. It is based on security frameworks, SOC 2 and NIST CSF, and has been adapted specifically for small business use. It is unlikely to be complete for your organization without customization. This document is not legal advice and I am independent of a registered CPA firm.

responsibilities, sets standards for prioritizing incidents, and establishes reporting and remediation procedures.

Our <Company Name> is committed to maintaining a culture of openness, trust, and integrity, especially when responding to security incidents. We're dedicated to protecting our employees, partners, and business from harmful actions, whether intentional or accidental.

Reporting Requirements: Any team member who suspects a theft, breach, or exposure of company data must immediately report it by:

Emailing: [insert designated email]
Calling: [company number]

2. Scope

This policy applies to all employees, contractors, and partners who handle our <Company Name>'s data, including personally identifiable information (PII) and other sensitive information. All vendor agreements must include clauses that align with these data protection standards.

3. Operational Incident-Handling Plan

<Company Name> employs an operational incident-handling capability that includes preparation, detection, analysis, containment, recovery, and user response activities.

Preparation

- Maintain updated inventory of IT assets and data
- Define clear roles and responsibilities for all team members and external resources
- Document contact information for all team members and external resources
- Establish secure communication channels for incident response
- Create and maintain incident response toolkit (templates, checklists)

Detection

- Monitor systems and networks for unusual activity
- Enable logging on all critical systems
- Implement alert thresholds for security events
- Educate staff on recognizing and reporting suspicious activities
- Regularly review security logs and alerts

Analysis

- Determine type of scope of incident
- Document the timeline of events
- Identify affected systems data

Disclaimer: This sample policy has been provided by Michael Nichols as a generic document to support the enhancement of your security posture. It is based on security frameworks, SOC 2 and NIST CSF, and has been adapted specifically for small business use. It is unlikely to be complete for your organization without customization. This document is not legal advice and I am independent of a registered CPA firm.

- Determine the potential impact to the business
- Classify incident severity (low, medium, high, critical)

Containment

- Isolate affected systems to prevent further damage
- Preserve evidence for analysis and potential legal requirements
- Change credentials for affected accounts
- Block malicious IP address or accounts

Recovery

- Clean and restore affected systems
- Verify systems are free of compromise before returning to production
- Implement additional security controls if necessary
- Monitor restored systems for any signs of persistent issues
- Document actions taken during recovery

User Response

- Notify affected individuals according to legal requirements
- Provide clear guidance on protective measures users should take
- Establish dedicated contact point for questions
- Document all communications with affected parties
- Follow-up with affected users as appropriate

4. Incident Tracking and Documentation

As soon as a theft, data breach or exposure containing <Company> Protected data or <Company> Sensitive data is identified, data relating to the incident must be documented and reported to both internal and external authorities.

- Use of incident tracking system [specify system] to record all incidents
- Document date, time, and description of the incident
- Record all actions taken in response
- Note team members involved in the response
- Track time spent on incident resolution
- Store evidence securely
- Document lessons learned

5. Incident Testing

<Company name> will test its incident response capabilities on a <insert frequency (ex: quarterly)> basis through:

Disclaimer: This sample policy has been provided by Michael Nichols as a generic document to support the enhancement of your security posture. It is based on security frameworks, SOC 2 and NIST CSF, and has been adapted specifically for small business use. It is unlikely to be complete for your organization without customization. This document is not legal advice and I am independent of a registered CPA firm.

- Tabletop exercises
- Simulated phishing attacks
- Incident response drills
- Post-exercise reviews to improve our procedures

6. Enforcement

Failure to comply with this policy may result in disciplinary action up to and including termination of employment. Third-party partners who violate this policy may have their access to <Company name> systems terminated.

7. Related Standards, Policies, and Processes

- Information Security Policy
- Acceptable Use Policy
- Data Classification Handling Policy
- Vendor Management Policy

8. Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

Term	Definition
Encryption or Encrypted Data	The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.
CUI (Controlled Unclassified Information)	Unclassified Information that should not be publicly disclosed
Personally Identifiable Information (PII)	Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered.
Safeguards	Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
Sensitive Data	A generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this

Disclaimer: This sample policy has been provided by Michael Nichols as a generic document to support the enhancement of your security posture. It is based on security frameworks, SOC 2 and NIST CSF, and has been adapted specifically for small business use. It is unlikely to be complete for your organization without customization. This document is not legal advice and I am independent of a registered CPA firm.