SMALL BUSINESS INFORMATION SECURITY 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.

[Company Name] Information Security Policy							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0							

1. Overview

This Information Security Policy establishes the foundation for protecting <Company Name>'s information assets and technology resources. It serves as the cornerstone of our security program, providing a framework that unifies and coordinates all our security efforts across the organization.

In today's digital business environment, information is one of our most valuable assets. This policy provides clear direction for preserving the confidentiality, integrity, and availability of our information assets, while ensuring business operations can continue efficiently and effectively.

2. Purpose

This policy establishes the overarching principles and requirements for protecting [Company Name]'s information assets. It provides a unified structure that connects our specific security policies into a comprehensive security program that balances protection with business needs.

3. Scope

This policy covers all technology used for business purposes, including:

- All employees, contractors, vendors, and partners who have access to <Company Name>'s information systems or data

- All information assets owned or managed by <Company Name>, regardless of location or format (electronic or physical)

- All technology systems and applications used for business purposes, whether company-owned or personally-owned (BYOD)

- All facilities where <Company Name> information is processed or stored

4. Information Security Governance

Roles and Responsibilities

Management

- Ultimate responsibility for information security resides with <Company Name>'s leadership
- Approve information security policies and significant changes
- Provide resources necessary to implement and maintain security controls
- Review security status reports and respond to significant issues
- Foster a culture of security awareness

Information Security Officer/Designee

- Develop and maintain information security policies and procedures
- Coordinate security activities across the organization
- Conduct or arrange security assessments and audits
- Monitor security incidents and responses
- Report on security status to management
- Serve as the primary point of contact for security matters

Department Managers

- Implement security controls within areas of responsibility
- Ensure staff understand and follow security policies
- Identify and report security issues
- Assist in data classification and risk assessment

All Users

- Comply with all information security policies and procedures
- Report security incidents and suspicious activities promptly
- Protect information assets under their control
- Participate in security awareness training
- Practice good security habits in daily activities

Security Decision-Making Process

- Security decisions balance protection needs with business requirements
- Risk-based approach guides priority of security investments
- Security considerations are integrated into business processes
- Clear escalation paths for security issues requiring management attention

5. Risk Management Approach

Risk Assessment Methodology

- Identify information assets and assign ownership
- Evaluate threats and vulnerabilities to assets
- Assess potential impact of security breaches on business operations
- Determine likelihood of security incidents
- Calculate risk levels based on impact and likelihood
- Prioritize risks based on business significance

Risk Treatment Options

- Risk Mitigation: Implement controls to reduce risk to acceptable levels
- Risk Acceptance: Formally accept risks that cannot be mitigated cost-effectively
- Risk Avoidance: Eliminate activities that create unacceptable risk
- Risk Transfer: Share risk through insurance or third-party services

Risk Acceptance Criteria

- Low risks may be accepted by department managers
- Moderate risks require approval from the Information Security Officer/Designee
- High risks require executive leadership approval
- Critical risks require board or owner approval
- All accepted risks must be documented with business justification

Review Frequency

- Formal risk assessments conducted annually
- Additional assessments after significant changes to systems or business operations
- Continuous monitoring for emerging threats and vulnerabilities
- Regular reporting of risk status to management

6. Policy Framework

This Information Security Policy serves as the umbrella document that unifies and coordinates the following supporting policies, creating a cohesive security program:

Supporting Policies

Acceptable Use Policy

Defines appropriate use of <Company Name>'s information systems and technology resources. Establishes user responsibilities and prohibited activities to maintain security and prevent misuse.

Data Classification & Handling Policy

Establishes a framework for classifying data based on sensitivity and defining appropriate controls for each classification level. Ensures consistent protection of information throughout its lifecycle.

Incident Response Policy

Outlines procedures for detecting, reporting, assessing, responding to, and recovering from security incidents. Minimizes damage from security breaches and enables swift, effective response.

Vendor Management Policy

Defines requirements for assessing, engaging, and monitoring third-party service providers who access, process, or store <Company Name>'s data. Ensures vendors maintain appropriate security controls.

Policy Maintenance

- All policies are reviewed at least annually
- Policies are updated in response to significant changes in business operations, technology, or threat landscape
- Version control maintained for all policy documents
- Policy changes are approved through established governance process

7. Compliance Requirements

Legal and Regulatory Requirements

- Privacy laws (e.g., CCPA, GDPR if applicable)
- Industry-specific regulations (e.g., HIPAA, PCI DSS if applicable)
- Data breach notification laws
- Employment and labor laws
- Intellectual property protection

Industry Standards

- ISO 27001 (as guidance)
- NIST Cybersecurity Framework
- Center for Internet Security (CIS) Controls
- Industry-specific security practices and guidelines

Contractual Obligations

- Customer agreements
- Business partner requirements
- Vendor contracts
- Insurance requirements

Compliance Monitoring

- Regular self-assessments against policy requirements
- Documentation of compliance evidence
- Remediation of identified gaps
- Reporting to management on compliance status
- Integration of compliance checks into business process

8. Asset Management

Effective asset management is essential for protecting <Company Name>'s information and technology resources:

Asset Inventory Requirements

- Maintain inventory of hardware, software, and information assets
- Record ownership, location, and purpose of assets
- Update inventory when assets are acquired, modified, or disposed

- Regularly verify inventory accuracy

Asset Ownership

- All assets have designated owners responsible for security
- Owners approve access rights and acceptable use
- Owners participate in risk assessments and classify data
- Owners ensure proper handling throughout asset lifecycle

Asset Classification

Assets are classified according to the Data Classification Policy:

- Restricted: Information whose unauthorized disclosure could cause significant harm
- Private: Information whose unauthorized disclosure could cause moderate harm
- Public: Information that can be freely disclosed

9. Access Control Principles

<Company Name> implements access controls based on the principle of least privilege:

Authentication Requirements

- Unique identification for all users
- Strong password requirements per Acceptable Use Policy
- Multi-factor authentication for sensitive systems or remote access
- Secure authentication protocols and mechanisms

Authorization Principles

- Access rights based on job requirements
- Formal approval process for access requests
- Regular review of access privileges
- Prompt removal of access when no longer needed

Least Privilege Approach

- Users granted minimum access needed for their roles
- Administrative privileges strictly limited
- Default deny for all access not explicitly authorized
- Separation of duties for critical functions

Access Review Process

- Managers review user access rights quarterly
- Access rights adjusted when roles change
- Immediate revocation when employment ends
- Documentation of all access reviews and changes

10. Security Awareness and Training

Building a security-conscious culture is essential to our information security program:

Training Requirements

- Security awareness training for all new users
- Annual refresher training for all users
- Role-specific security training as needed
- Training on new security threats and controls

Frequency of Training

- Initial training during onboarding
- Annual refresher courses
- Additional training after significant security incidents
- Updates when policies or procedures change

Awareness Program Components

- Regular communications about security topics
- Simulated phishing exercises
- Security reminders and tips
- Reporting mechanisms for security concerns

Measuring Effectiveness

- Knowledge assessments after training
- Tracking of security incidents related to user behavior
- Monitoring policy compliance
- Feedback collection to improve training

11. Security Incident Management

<Company Name> maintains procedures for managing security incidents efficiently and effectively, with details documented in the Incident Response Policy:

High-Level Incident Response Approach

- Preparation: Maintaining readiness for security incidents
- Detection and Analysis: Identifying and evaluating potential incidents
- Containment: Limiting damage from confirmed incidents
- Eradication: Removing the cause of the incident
- Recovery: Restoring systems to normal operation
- Post-Incident Activities: Learning from incidents to prevent recurrence

Breach Notification Requirements

- Internal reporting procedures and escalation paths
- External notification requirements per applicable laws
- Customer and partner communication procedures
- Documentation of notification decisions and actions

Escalation Paths

- Initial incident reporting to designated security contacts
- Severity-based escalation to management
- Engagement of external expertise when needed
- Communication with legal counsel for significant incidents

12. Business Continuity

<Company Name> prepares for disruptions to ensure continuous operation of critical business functions:

Connection to Business Continuity Planning

- Information security integrated with business continuity planning
- Security considerations in disaster recovery procedures
- Backup and restoration processes for critical data
- Alternate processing capabilities for essential systems

Recovery Time Objectives

- Defined recovery timeframes based on business impact
- Prioritization of systems and data for restoration
- Regular testing of recovery capabilities
- Documentation of recovery procedures

Critical Systems and Processes

- Identification of systems essential for business operations
- Enhanced protection for mission-critical assets
- Redundancy for key infrastructure components
- Alternative procedures for when systems are unavailable

13. Enforcement

Compliance with this policy and supporting policies is mandatory for all users:

Consequences for Non-Compliance

- Violations may result in disciplinary action up to and including termination
- Severity of consequences proportional to the violation and resulting harm
- Consistent application of enforcement actions
- Legal action for severe violations causing significant harm

Disciplinary Procedures

- Initial notification and education for minor violations
- Formal warnings for repeated or more serious violations
- Temporary suspension of access privileges when appropriate
- Documentation of all enforcement actions

Exceptions Process

- Formal process for requesting policy exceptions
- Business justification required for all exceptions
- Approval authority based on risk level
- Regular review of granted exceptions
- Documentation of all exceptions

14. Policy Review

To maintain effectiveness, this policy will be regularly reviewed and updated:

Review Frequency

- Annual review of all information security policies
- Additional reviews after significant security incidents
- Updates in response to major changes in business operations or technology
- Constant monitoring for changes in compliance requirements

Approval Process

- Updates proposed by Information Security Officer/Designee
- Review by affected stakeholders
- Approval by management or security committee
- Distribution to all users

Version Control

- Documented revision history for all policies
- Clear marking of current version and effective date
- Archive of previous policy versions
- Communication of significant changes

Change Management

- Impact assessment for policy changes
- Appropriate notice before implementing changes
- Training or communication on significant changes
- Transition period for implementing new requirements

15. Related Standards, Policies, and Processes

The following documents support and extend this Information Security Policy:

- Acceptable Use Policy
- Data Classification and Handling Policy
- Incident Response Policy
- Vendor Management Policy

16. Definitions and Terms

Term	Definition
Confidentiality	Ensuring that information is accessible only to those authorized to have access
Integrity	Safeguards the accuracy and completeness of information
Availability	Ensuring that authorized users have access to information when required
Information Asset	Any information that has value to the organization
Information Security	Preservation of confidentiality, integrity, and availability of information
Risk	Effect of uncertainty on objectives, measured in terms of likelihood and impact
Security Incident	A single or series of unwanted events that compromise business operations or security
Vulnerability	A weakness that can be exploited by threats to harm the organization
Threat	Potential cause of an unwanted incident that may result in harm to the organization