SB InfoSec Policy Starter Kit - Introduction Guide

About This Resource

Welcome to your free Information Security Policy Starter Kit! This resource is designed to help small businesses establish fundamental security policies without the need for specialized IT expertise or expensive consulting services.

Why These Policies Matter

Small businesses are increasingly targeted by cybercriminals because they often lack formal security programs. Having these policies in place will:

- Protect your valuable business data
- Reduce the risk of costly security incidents
- Build trust with customers and partners
- Provide a foundation for compliance requirements
- Create consistent security practices across your organization

What's Included in This Kit

This kit contains five essential security policies that every small business should have:

1. **Information Security Policy**
    - The foundation of your security program
    - Outlines general principles and responsibilities
    - Establishes your security governance structure

2. **Acceptable Use Policy**
    - Defines proper use of technology resources
    - Clarifies expectations for employee behavior
    - Helps prevent security incidents caused by misuse

3. **Data Classification & Handling Policy**
    - Creates a framework for categorizing sensitive data
    - Establishes handling requirements for each category
    - Ensures appropriate protection of valuable information
4. **Vendor Management Policy**
    - Guidelines for assessing and monitoring third parties
    - Reduces risks from external service providers
    - Protects your data when shared with vendors
5. **Incident Response Policy**
    - Procedures for responding to security breaches
    - Clarifies roles and responsibilities during incidents
    - Helps minimize damage when security events occur

How to Use This Kit

Step 1: Review and Customize (Week 1)

- Read through each policy and understand its purpose
- Replace all [Company Name] placeholders with your business name
- Adjust specific sections to fit your business size and industry
- Consider your current practices and realistic capabilities

Step 2: Prioritize Implementation (Week 2)

1. Start with the Acceptable Use Policy - this affects daily operations
2. Implement Information Security Policy - establishes your foundation
3. Apply Data Classification Policy - organizes your information
4. Adopt Vendor Management Policy - secures external relationships
5. Establish Incident Response Policy - prepares for security events

Step 3: Communicate with Your Team (Week 3)

- Schedule a meeting to introduce the policies
- Focus on explaining the "why" behind security measures
- Provide practical examples relevant to daily work

- Address questions and concerns openly
- Document acknowledgment of policies

Step 4: Create Simple Monitoring System (Week 4)

- Set calendar reminders for regular security activities
- Create basic checklists for security practices
- Establish a point of contact for security questions
- Plan quarterly review sessions to discuss security

Security Resources for Small Businesses

Free Tools

- CISA Cyber Essentials: www.cisa.gov/cyber-essentials
- FTC Cybersecurity for Small Business: www.ftc.gov/business-guidance/small-businesses/cybersecurity
- Small Business Administration Resources: www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity

Monthly Security Habits

- Schedule 15 minutes on the first Monday of each month to discuss security
- Verify that system updates have been installed across all devices
- Check that backups are running properly
- Review and address any security concerns from employees

Implementation Quick Tips

Getting Started Immediately

1. **Day 1**: Read through all policies to understand the scope
2. **Day 2-3**: Customize policies with your company name
3. **Day 4-5**: Identify 3-5 security improvements you can make this week
4. **Week 2**: Introduce policies to your team in a brief meeting
5. **Week 3-4**: Implement one policy per week, starting with Acceptable Use

Security Basics Every Business Should Implement

- Enable automatic updates on all devices
- Use strong, unique passwords for all business accounts
- Turn on multi-factor authentication for critical services
- Back up important business data regularly

- Use antivirus/security software on all devices
- Train employees to recognize phishing attempts

About the Author

This starter kit has been provided by Michael Nichols, an Information Security Professional specializing in security frameworks, SOC 2, and NIST CSF implementation. Michael focuses on making security practical and accessible for small businesses.

Contact Information:

- Email: manichols936@gmail.com
- LinkedIn: Connect with Michael on LinkedIn for professional networking

---

Disclaimer: This starter kit has been provided 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 the author is independent of a registered CPA firm.