SMALL BUSINESS ACCEPTABLE USE 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><th colspan="8">[Company Name]
Acceptable Use Policy</th></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. Overview....3
2. Purpose.... 3
3. Scope.... 3
4. Policy....3
    4.1 General Use and Ownership.... 3
    4.2 Security & Proprietary Information....4
    4.3 Unacceptable Use.... 4
    4.3.1 System and Network Activities.... 5
    4.3.2 Email and Communication Activities.... 5
    4.3.3 Blogging and Social Media.... 5
5. Policy Compliance....6
    5.1 Compliance Measurement....6
    5.2 Exceptions....6
    5.3 Non-Compliance....6
6. Implementation Guide.... 6
    6.1 Quick Start Actions....6
    6.2 Monthly Security Habits....7
    6.3 Security Resources for Immediate Use.... 7

1. Overview

Effective security doesn't require a large IT team or complex systems. This policy

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.

helps <Company Name> personnel protect their valuable information with straightforward guidelines that anyone can follow. By implementing these basic rules, <Company Name> can significantly reduce security risks while maintaining productivity.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy explains the proper use of computers, mobile devices, and network resources of <Company Name>. Following these guidelines protects both <Company Name> and its personnel from security threats like malware, data breaches, and legal problems that could disrupt operations or damage their reputation.

3. Scope

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

- Company-owned computers and devices

- Personal devices used for work (BYOD)

- Internet connections and email accounts used for business

- Cloud services and applications

All personnel who work with <Company Name> should follow these guidelines, including full-time employees, part-time staff, contractors, and temporary workers.

4. Policy

4.1 General Use and Ownership

4.1.1 <Company Name> business information stored on electronic and computing devices whether owned or leased by <Company Name>, the employee or a third party, remains the sole property of <Company Name>. You must ensure through legal or technical means that business information is protected.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of <Company Name> proprietary information.

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.

4.1.3 You may access, use or share <Company Name> proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Limited personal use of business technology is permitted as long as it doesn't interfere with work responsibilities, consume significant resources, or introduce security risks. When in doubt, ask before using business technology for personal matters.

4.1.5 <Company Name> reserves the right to monitor systems and network activity to ensure security and proper use. This may include reviewing web browsing history, email communications, and file storage when necessary for security or troubleshooting purposes.

4.2 Security & Proprietary Information

4.2.1 All mobile and computing devices that connect to the business network must be up-to-date security protections including antivirus software and current security updates.

4.2.2 All passwords must be strong and unique, containing a mix of letters, numbers, and special characters. Never share passwords or provide access to your account to others.

4.2.3 All computing devices must be secured with a password-protected screensaver that activates after 10 minutes or less of inactivity. Always lock your screen or log off when leaving your device unattended.

4.2.4 When using a company email address in online discussions or social media, include a disclaimer stating that opinions expressed are your own and not necessarily those of the business, unless posting as an official representative.

4.2.5 Exercise extreme caution when opening email attachments or clicking links, especially from unknown senders, as they may contain malware or phishing attempts. When in doubt, verify the source before proceeding.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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.

1. Installing or sharing unauthorized software, media, or other content protected by intellectual property laws.

2. Accessing data, accounts, or systems for purposes other than conducting <Company Name>business, even if you have the access to do so.

3. Disrupting network communications, scanning for vulnerabilities without authorization, or monitoring network traffic outside of your job responsibilities.

4. Uploading malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Sharing your account password with others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.3.2 Email and Communication Activities

When using company resources to access/use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

1. Sending unsolicited messages, “junk” mail”, or advertisements to individuals who haven't requested such material.

2. Any form of harassment via email, messaging, or other communication channels, regardless of language, frequency, or message size.

3. Forging email headers or sender information, or impersonating others in communications.

4. Creating or forwarding chain letters, pyramid schemes, or similar unauthorized mass communications.

5. Using business email or messaging systems for extensive personal correspondence or non-business activities within <Company Name>’s networks of other internet/intranet/extranet service providers.

4.3.3 Blogging and Social Media

1. Revealing business confidential information, trade secrets, or proprietary data on blogs, social media, or other online platforms.

2. Posting content that could harm the business's reputation, including discriminatory, defamatory, or harassing comments.

3. Representing personal opinions as official business statements or positions without authorization.

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.

4. Using business logos, trademarks, or brand identity in unauthorized ways or in connection with personal online activities.

5. Engaging in extensive social media or blogging activities during work hours that interfere with job responsibilities.

5. Policy Compliance

5.1 Compliance Measurement

Compliance with this policy will be verified through regular discussions during team meetings, occasional review of system activities, and informal workplace observations. The goal is to ensure the policy is understood and followed, not to strictly monitor employees.

5.2 Exceptions

Exceptions to this policy may be granted when necessary for business operations. All exceptions should be discussed with and approved by business leadership before proceeding.

5.3 Non-Compliance

Failure to comply with this policy may result in:

1. Additional security awareness coaching
2. Temporary restriction of technology privileges
3. Disciplinary action appropriate to the severity of the violation

6. Implementation Guide

6.1 Quick Start Actions

- Schedule a 30-minute meeting to review key points with all staff and have everyone acknowledge that they've read and understood it
- Post reminders about key points in visible locations
- Verify all devices have the following to ensure basic security:
    - Automatic updates enabled (set aside 1 hour this month to check all devices)
    - Current antivirus/antimalware protection installed
    - Password-protected screensavers activated
- Post reminders about key points in visible locations
- Consider Implementing a free or low-cost password manager to maintain strong passwords
- Set up automatic backups for critical business information (at minimum, weekly backups of essential files)
- Document Recovery Plan Create a simple one-page document listing steps to take if a device is lost/stolen or if you suspect a security breach

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.

6.2 Monthly Security Habits

- Set aside 15 minutes on the first Monday of each month to discuss any security concerns
- Check that all system updates have been applied
- Verify backups are working properly by testing a file recovery
- Review any unusual activities or potential policy violations

6.3 Security Resources for Immediate Use

- FCC Cyberplanner: www.fcc.gov/cyberplanner (10-minute assessment to create a custom plan)
- CISA Small Business Resources: www.cisa.gov/small-business (free tools and guides)
- Small Business Administration Cybersecurity Portal: www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity (step-by-step implementation guidance)

6. Related Standards, Policies, and Processes

- Information Security Policy
- Data Classification Handling Policy
- Vendor Management Policy
- Incident Response Policy

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.