# SMALL BUSINESS CYBERSECURITY POLICY

Essential Edition — Free Template

Provided by SmallBizSecurityGuide.com | Based on NIST CSF 2.0 & CISA Cyber Essentials

| | |
|---|---|
| **Business Name** | _____ |
| **Effective Date** | _____ |
| **Policy Owner** | _____ |
| **Review Date** | _____ |

This policy applies to all employees, contractors, and third parties who access company systems, networks, or data. All personnel must read and sign this policy before accessing company systems.

## 1. ACCEPTABLE USE

- Company devices and systems are for business use. Limited personal use is permitted if it does not interfere with work or create security risk.
- Do not install unauthorized software on company devices. All software must be approved by the owner or IT manager.
- Do not access inappropriate, illegal, or harmful content using company systems or networks.
- Company systems and accounts may be monitored. Employees have no expectation of privacy on company-owned equipment.
- Do not use company email or systems for personal business, side ventures, or activities that could create legal liability.

## 2. PASSWORDS & ACCESS

- All passwords must be at least 14 characters. Use a passphrase — three or more random words — rather than complex short passwords.
- Never share passwords with anyone, including IT support or managers. No legitimate IT request will ask for your password.
- Use a different password for every system and account. Use the company password manager to store them.
- Multi-factor authentication (MFA) is required on all email accounts and any system accessible from the internet.
- Change passwords immediately if you suspect they have been compromised. Report the incident to the owner.

## 3. DATA PROTECTION

- Customer data, financial records, and employee information are confidential. Do not share them outside the company without authorization.

- Do not store confidential business data on personal devices, personal email, or unauthorized cloud services.
- Encrypt sensitive files before emailing them. When in doubt, ask before sending.
- Lock your computer screen when stepping away from your desk — Windows + L or Command + Control + Q on Mac.
- Shred printed documents containing customer or financial information. Do not put them in the recycling bin.

## 4. PHISHING & SUSPICIOUS ACTIVITY

- Do not click links or open attachments in unexpected emails — even from known senders. When in doubt, call the sender to verify.
- Check the actual sender email address, not just the display name. Attackers fake display names to look legitimate.
- Never wire money, purchase gift cards, or change payment information based on an email request without voice confirmation.
- If you think you clicked something suspicious — report it immediately. You will not be blamed for reporting. Silence makes breaches worse.

## 5. INCIDENT REPORTING

- Report any suspected security incident immediately — lost device, suspicious email, unusual system behavior, or unauthorized access.
- **Report to:** _____ Phone: _____
- Do not attempt to investigate or resolve a security incident on your own. Contain it — isolate the device from the network if possible — then report.
- Violations of this policy may result in disciplinary action up to and including termination.

## EMPLOYEE ACKNOWLEDGMENT

I have read, understood, and agree to comply with this Cybersecurity Policy. I understand that violations may result in disciplinary action.

**Employee Name (Print)** _____

**Date** _____

**Employee Signature** _____

**Manager Signature** _____