SMB Security Policy Pack - Short Form (Sample)

Lightweight, plain-English policies designed for small teams. Customize names, tools, and owners.

How to use: assign an owner per policy, review quarterly, and keep evidence (screenshots/logs) in a shared folder.

1) Access and Identity (MFA + admin separation)

Purpose: Prevent account takeover from becoming company takeover.

Owner: IT/Admin Lead | **Review:** Quarterly

- • All accounts use MFA (or passkeys) where supported; admins are mandatory.
- • Admin accounts are separate from daily work accounts (no browsing/email on admin).
- • Vendor access is named, MFA-protected, time-bound, and logged.
- • Break-glass accounts exist (2). Credentials stored offline and tested quarterly.
- • Offboarding happens within 24 hours of departure.

2) Backups and Recoverability (3-2-1, test restores)

Purpose: Ensure the business can recover from ransomware, deletion, and mistakes.

Owner: IT/Admin Lead | **Review:** Quarterly

- • Use 3-2-1: 3 copies, 2 different media, 1 offline/immutable copy.
- • Backup admin credentials are different from everyday admin credentials.
- • Define top 3 critical systems with target RTO/RPO and owners.
- • Run a quarterly restore drill and store evidence (timings + screenshots).
- • Review backup failures weekly.

3) Device Baseline (patching + encryption + least privilege)

Purpose: Reduce the blast radius of phishing and malware.

Owner: Operations / IT | **Review:** Quarterly

- • Patch OS and key apps within 14 days (critical faster).
- • Enable full-disk encryption on all company laptops.
- • Users do not have local admin rights by default.
- • Security software (AV/EDR) must be installed and active.
- • Lost/stolen devices reported within 2 hours; remote wipe if possible.

4) Incident Response (first hour actions)

Purpose: Contain incidents quickly and preserve evidence for recovery and insurance.

Owner: Incident Lead | **Review:** After any incident + quarterly

- • If ransomware suspected: isolate affected device(s) immediately (disconnect network).
- • Disable suspected accounts; rotate credentials and revoke tokens.
- • Capture evidence (screenshots/logs) before cleanup.
- • Notify the incident lead and business owner within 30 minutes.
- • Follow the recovery drill runbook to validate restores.

Appendix A - Evidence checklist

- [] MFA proof (admin + users) and sign-in logs
- [] Admin separation proof and privilege review
- [] Backup job success + immutable/offline configuration
- [] Quarterly restore drill report (RTO/RPO measured)
- [] Vendor access list with expiry dates
- [] Asset inventory updated monthly

For audit-grade versions aligned to ISO 27001 / NIST CSF / DORA, we provide the extended pack to subscribers.