Small Business Security Policy Template

Template · Minimum Security Policy For 1–25 Employee Businesses.

A starter policy covering the essentials. Customise the bracketed sections, have all employees sign, review annually. Pair with cyber-insurance underwriting requirements.

1. Purpose & Scope

This policy describes the minimum security practices required of all employees, contractors, and authorised users of [Company Name]'s systems and data.

Effective date: _____ · Policy owner: _____

2. Acceptable Use

- Company devices are for business use plus reasonable personal use that does not introduce risk.
- No installation of unauthorised software on company devices.
- No sharing of credentials, including with co-workers.
- No use of public Wi-Fi for sensitive work without approved VPN.
- Lost or stolen devices must be reported immediately.

3. Password & Authentication

- All employees use the company password manager: [Manager Name].
- MFA is required on email, financial systems, admin tools, and customer-facing systems.
- Authenticator-app MFA is preferred over SMS.
- Recovery codes for shared accounts are stored in [secure shared vault].

4. Device Security

- All laptops have full-disk encryption (FileVault on Mac, BitLocker on Windows).
- Auto-updates enabled for OS, browsers, and productivity software.
- Endpoint protection (antivirus or EDR) running on every device.
- Screen lock with passcode after 5 minutes of inactivity.
- Personal devices (BYOD): require MDM enrolment if used for company email.

5. Email & Communication

- Suspicious emails reported to [phishing report channel] — do not click, do not reply.
- Wire-transfer requests verified out-of-band (callback to a known number) before action.
- Sensitive customer data not sent over unencrypted email.

6. Data Protection

- Customer data classified as sensitive — encrypted at rest and in transit.
- Data retention: customer records kept for [X] years, then deleted.
- Backups follow 3-2-1 — daily, automated, tested quarterly.
- Personal data handling complies with [applicable privacy laws].

7. Incident Reporting

Any suspected security incident must be reported immediately to [security contact] via [email / phone]. The Incident Response Plan applies.

8. Vendor Risk

- New vendors with access to company data go through [security review process].
- Vendor list maintained at [location] with security review notes.
- Annual review of all vendors' security posture.

9. Training

All employees complete [security awareness training] within [X] days of hire and annually thereafter.

10. Acknowledgement

I have read and agree to follow this policy.

Employee name: _____ Date: _____

Signature: _____