



Cybersecurity Policy

One-page baseline policy · SMB1001 Control 21 · Replace [bracketed] items with your details.

[Business name] takes the security of our systems, our money and our customers' information seriously. This policy sets the basic rules everyone who uses our systems must follow. It applies to all staff, contractors and anyone with access to our accounts or devices.

Our rules

- **Accounts.** Every person has their own login. We never share accounts or passwords.
- **MFA.** Multi-factor authentication (MFA) is switched on for email and every important system.
- **Passwords.** We use a password manager to create and store long, unique passwords.
- **Updates.** Automatic updates are on for computers, phones and key software.
- **Backups.** Business data is backed up automatically, with one copy kept offline or isolated, and restores are tested.
- **Payments.** Any change to a supplier's bank details is verified by phone using a known number before we pay. Urgency is a red flag, not a reason to skip a step.
- **Reporting.** Anyone who sees, or realises they've clicked, something suspicious reports it straight away. There is no blame for honest mistakes — we need to know quickly.
- **Joiners and leavers.** Accounts and access are set up on a person's first day and removed on their last day.

Who owns this

Policy owner (name / role): _____

IT support / provider: _____

Reviewed (date): ____ / ____ / ____ Next review: _____

This policy is reviewed at least once a year and after any significant incident.

Make it yours (with AI)

I run a [type of business] in [town], Australia, with [number] staff. Rewrite the policy below so it fits how my business actually works, in plain English my team will read. Keep it to one page. [paste the template]

Two rules: start a fresh chat, and never paste real customer names, bank details or staff records into a free AI tool.