



Small Business Cybersecurity Checklist

A practical review of the security basics every small business should have in place, from MFA and patching to backups and incident contacts.

Work through each item with the person who manages your IT. Tick an item only when you have checked it is actually in place, not when you believe it probably is. Record anything that needs attention in the follow-up actions table on the last page.

Business name

Review date

Reviewer

Next review due

Recommended practice, not formal compliance

Every item in the main checklist is a **recommended good practice** for small businesses. Completing it does not make your business compliant with any law, standard or contract. Formal requirements, such as privacy obligations, industry rules, insurer conditions or an Essential Eight maturity assessment, must be checked separately. Use the short list at the end of this checklist as a starting point.

Accounts and access

Done	Item
☐	Multi-factor authentication (MFA) is enabled on important accounts Email, Microsoft 365 or Google Workspace, banking, accounting, payroll, domain and website accounts.
☐	Every account uses a strong, unique password No password is reused across services. Long passphrases are easier to remember and harder to guess.
☐	A password manager is used to store business passwords Staff use an approved password manager rather than spreadsheets, notebooks or browser notes.
☐	Administrator access is reviewed Only people who need administrator rights have them, and they use a separate standard account for everyday work.

Devices and software

Done	Item
☐	Windows and applications are kept up to date Automatic updates are on, and someone checks that updates are actually installing on every device.
☐	Endpoint protection is installed and active Antivirus or endpoint detection is running, up to date and monitored on every computer.
☐	Devices are encrypted BitLocker (Windows) or FileVault (Mac) is on for laptops and computers that hold business data. Phones use a passcode.

Done	Item
☐	Remote access is secured Remote desktop and VPN access require MFA, are limited to the people who need them and are not exposed directly to the internet.

Email, data and people

Done	Item
☐	Email security is configured Spam and phishing filtering are on, and your domain has SPF, DKIM and DMARC records set up.
☐	Backups are configured for important data Business files, email and key systems are backed up automatically, with at least one copy kept separate from your main systems.
☐	Backup restoration has been tested You have actually restored files from a backup recently. A 'backup successful' message alone does not prove you can recover.
☐	Staff receive security awareness training Staff know how to spot phishing, unexpected payment requests and suspicious MFA prompts, and how to report them.

Preparedness

Done	Item
☐	Incident response contacts are recorded Everyone knows who to call if something goes wrong: your IT provider, bank, insurer and key internal contacts.
☐	Security is reviewed periodically This checklist, or a fuller review, is repeated at least every six to twelve months and after major changes.

Formal requirements to check separately

These are not part of the recommended practices above. Tick each one once you have confirmed whether it applies to you.

Done	Requirement
☐	Privacy obligations Whether the Privacy Act 1988 and the Notifiable Data Breaches scheme apply to your business.
☐	Industry or sector rules Requirements from regulators or professional bodies in your industry.
☐	Contract and supplier conditions Security clauses in customer, government or supplier contracts.
☐	Cyber insurance conditions Controls your insurer requires, such as MFA or tested backups, for a claim to be valid.

Follow-up actions

Action needed	Responsible person	Target date	Completed

Need a hand?

Omnicon I.T. Services can help you put this into practice. Visit omnicron.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicron.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.