AgileIT

Family-owned managed IT since 2007 | Melbourne & Mornington Peninsula

A CYBER SECURITY CHECKLIST FOR AUSTRALIAN SMBs

The Mornington Peninsula SMB Cyber Security Checklist

Eight categories. Around fifty checkpoints. A practical scorecard for any small or medium business in Melbourne or the Mornington Peninsula that wants a clear, honest read on where it sits today.

How to use this checklist

Work through each section honestly. Tick the items you can confidently say are in place and working today. Leave the others blank. Total your ticks at the end. The result is not a grade, it is a starting position. The aim is to know where you stand, not to score well.

Prepared by Agile IT Solutions. Family-owned managed IT, cyber security and AI enablement for Australian SMBs since 2007. Founding member of SMBiT Professionals. Microsoft AI Cloud Partner.

Why this checklist

Cyber security guidance written for enterprises does not fit a 15-person professional services firm in Frankston or a 40-person practice in Brighton. The advice is correct in principle, but the controls assumed (dedicated security teams, budgets in the hundreds of thousands, mature compliance functions) do not exist in most SMBs.

This checklist is the Australian SMB version. It assumes one director who carries the risk, a small team that uses IT to do client-facing work, a managed Microsoft 365 environment, and a budget that has to make sense against the rest of the business. Every item is something we have seen make a real difference for businesses of that profile.

How the checklist is organised

Eight categories, each addressing one area of the business:

01	**Identity and access**	The accounts that protect everything else
02	**Devices and endpoints**	Every laptop and phone is a potential entry point
03	**Email and phishing**	Still the most common delivery mechanism
04	**Data and backups**	A working backup is not the same as a tested restore
05	**Network and connectivity**	The perimeter is more porous than it used to be
06	**Vendors and third parties**	A breach at a supplier becomes your breach
07	**Incident readiness**	Decide how you respond before it happens
08	**Governance and culture**	Cyber is a business risk, not an IT problem

Each item is written so the answer is yes or no, not a percentage or maybe. If you cannot confidently say yes, treat it as a no for now. Honesty is more useful than a high score.

01 Identity and access

Most cyber incidents in Australian SMBs start with a compromised account, not a clever zero-day. Get this section right and you have closed off the most common attack path.

- **Multi-factor authentication is on for every business account**
  Microsoft 365, Google Workspace, line-of-business apps, finance systems, social media. No exceptions for owners or executives.
- **A password manager is in use across the business**
  No shared passwords in spreadsheets or sticky notes. Generated passwords, unique per service.
- **There is a defined leavers process**
  Same-day account disablement, device wipe, password rotation for anything shared. Written down, not improvised.
- **Privileged accounts are separated from daily-use accounts**
  Administrators have a second account for admin work. Daily browsing and email use the standard account.
- **Inactive accounts are removed quarterly**
  Old contractor, intern, ex-staff, ex-vendor logins. Reviewed and removed on a schedule.
- **Conditional access policies are in place**
  Sign-in from unfamiliar countries blocked or challenged. Managed-device-only access for sensitive systems where it fits.

02 Devices and endpoints

Every laptop and phone in the business is a potential entry point. Modern endpoint management is the difference between a stolen laptop being an inconvenience and a stolen laptop being a breach.

- **Full-disk encryption is enabled on every business device**
  BitLocker on Windows, FileVault on macOS. Confirmed, not assumed.
- **Endpoint detection and response (EDR) is deployed**
  Microsoft Defender for Business or equivalent. Going beyond free antivirus is the standard for any business handling client data.
- **Operating systems and applications are patched within 14 days**
  Critical security updates inside two weeks of release. Automated where possible, audited monthly.
- **A mobile device management platform is in use**
  Microsoft Intune or equivalent. Devices enrolled. Lost-device wipe possible without involving the user.

- **USB and removable media policies are set**
  Either blocked or restricted to encrypted, business-approved devices.
- **A documented device inventory exists**
  Asset register kept current. Includes who has what and which devices are managed.

03 Email and phishing

Email is still the most common delivery mechanism for ransomware and business email compromise. The technical controls and the team training matter equally.

- **SPF, DKIM and DMARC are configured on your domain**
  Stops attackers spoofing your business email. DMARC set to at least quarantine, ideally reject.
- **Advanced threat protection is enabled in Microsoft 365 or equivalent**
  Safe Attachments and Safe Links if you are on Business Premium. Sandboxing for unknown attachments.
- **Anti-impersonation rules are in place for your executives**
  Microsoft 365 anti-phishing rules to detect spoofed sender names and lookalike domains.
- **Staff have completed phishing awareness training in the last 12 months**
  Not a one-time induction. Refreshed annually with simulated phishing campaigns.
- **There is a one-click way for staff to report a suspicious email**
  A Report button in Outlook, or a dedicated mailbox. Reports are reviewed, not lost.
- **Banking and finance approvals require a callback for changes**
  Voice verification on any new payee, bank-detail change, or unusual payment request. Even when the email looks legitimate.

04 Data and backups

A working backup is not the same as a tested restore. Most ransomware-affected businesses discover the difference at the worst possible moment.

- **Critical business data is backed up at least daily**
  Microsoft 365 data is not backed up by Microsoft. You need a third-party backup tool for email, OneDrive, SharePoint, Teams.
- **At least one backup copy is offsite or immutable**
  3-2-1 backup rule. Three copies, two media, one offsite. Immutable copies survive ransomware that targets the backup itself.
- **A full restore was tested in the last 6 months**
  Real restore, not a backup-job report. Documented outcome, including how long it took.

- **A data inventory exists for sensitive information**
  You know what client information, financial records, and regulated data you hold, and where it lives.
- **Document sharing is reviewed quarterly**
  External sharing on SharePoint and OneDrive audited. Old shared links removed.
- **A retention policy is documented and applied**
  You know how long you keep what, and old data is deleted on a schedule.

05 Network and connectivity

Your network is the perimeter, and it is increasingly porous. Remote workers, BYOD, IoT devices and guest visitors all change the shape of what you are defending.

- **A business-grade firewall is in place at every office**
  Configured, monitored, and reviewed. Not a consumer router.
- **Guest Wi-Fi is on a separate network**
  Isolated from business systems. Visitors get internet, not access to your network.
- **Remote access uses MFA and conditional access**
  No flat VPN that gives full network access from anywhere with a password. Zero-trust principles where possible.
- **Network segmentation separates user devices from servers and IoT**
  Workstations, servers, printers, cameras and IoT devices on separate VLANs.
- **Firmware on network equipment is updated**
  Switches, firewalls, access points. Updates reviewed and applied on a schedule.
- **Network diagrams and inventory are current**
  You or your provider can produce a diagram of the network in 10 minutes, not a week.

06 Vendors and third parties

A breach at a supplier becomes your breach if their access to your systems is not managed. This is the area most often overlooked in SMB security reviews.

- **A current list of third parties with access to your systems exists**
  Accountant, bookkeeper, marketing agency, IT provider, software vendors. Reviewed annually.
- **Third-party access uses MFA and unique accounts**
  No shared logins. Removed when the engagement ends.

- **A software inventory is kept current**
  You know what is installed across the business. Unused or unsupported software is identified and removed.
- **Cyber security due diligence is part of vendor selection**
  Before a new supplier touches client data, they answer security questions. Not after.
- **Cloud service permissions are reviewed quarterly**
  Third-party apps connected to Microsoft 365 or Google Workspace are reviewed and revoked where unnecessary.

07 Incident readiness

Decide how you respond before something happens, not while it is happening. A clear plan turns a potential disaster into a manageable interruption.

- **A written incident response plan exists**
  Covers ransomware, phishing compromise, data loss, lost device. Updated annually.
- **Contact list for an incident is current**
  Your IT provider, cyber insurance broker, legal contact, communications lead. On paper as well as digital, in case email is down.
- **Cyber insurance is in place and current**
  Reviewed annually with your broker. Coverage matches your actual risk and revenue.
- **Reporting paths are known**
  ReportCyber (cyber.gov.au) for incidents. OAIC for notifiable data breaches. Documented in your plan.
- **A post-incident review process is defined**
  After every incident or near-miss, the team meets to review and update the plan.

08 Governance and culture

Cyber security is a business risk, not an IT problem. The businesses that handle it best treat it that way.

- **A named owner inside the business is accountable for cyber security**
  Usually a director or senior manager. Not your IT provider.
- **The business is aligned to a recognised framework**
  SMB1001, the ASD Essential Eight, or NIST. A framework gives a measurable starting point.
- **A cyber security item appears in board or leadership meetings**
  Not every meeting, but at least quarterly. Reviewed at the same level as financial risk.

- **Staff complete an annual security refresher**
  Beyond phishing training. Covers handling client data, working from home, reporting concerns.
- **A current cyber risk register exists**
  Top risks identified, ownership assigned, mitigation in place or planned.
- **A budget exists for cyber security**
  It is a line item, not a surprise. Reviewed annually as part of the IT budget.

Your score, and what it means

Count the boxes you have ticked. Use the table below to interpret the result.

Range	Interpretation
Below 20	Significant exposure. Most controls are missing or inconsistent. Cyber security is being managed reac
20 to 30	Partial maturity. Some good practice in place, but gaps that an opportunistic attacker would find. A stru
31 to 40	Solid foundation. The basics are in place and the business is on the front foot. Worth refining the more
41 to 50+	Strong posture. Most controls are mature. The work now is keeping them current, training the team, ar

What to do with the result

The point of the checklist is not the number. The point is the conversation it makes possible. Inside your business, the score gives the team a clear starting position. In a conversation with a managed IT provider, it gives you something to compare quotes against. In a conversation with your insurer, it shows you have looked, deliberately, at where you stand.

Most businesses sit somewhere between 20 and 35 on their first run-through. That is normal. The plan to move from 25 to 40 over the next year is more valuable than a one-off score.

Want a second pair of eyes on the result?

Agile IT runs a free 45-minute Cyber Health Check conversation. We walk through your checklist result together, talk through what is on your radar, and give you an honest read on where the meaningful gaps are. No quote pushed, no obligation.

Book a Cyber Health Check at agileit.com.au/cyber-health-check/
or call 1300 859 910 and ask for the team.

About Agile IT Solutions

Agile IT is a family-owned managed IT, cyber security and AI enablement business, founded in 2007. We work with small and medium businesses across Melbourne and the Mornington Peninsula. Our service is delivered through the AgileMANAGED platform: one accountable partner across IT support, cyber security, AI, business voice and connectivity.

We are a founding member of SMBiT Professionals, the Australian peak body for managed IT services serving the SMB market. We are a Microsoft AI Cloud Partner. Our security work is aligned to the SMB1001 framework and the ASD Essential Eight.

How we work

Every engagement starts with a discovery conversation, either on-site or via Microsoft Teams. It is 45 to 60 minutes, free of charge, structured around five themes, and ends with you in control of the next step. There is no quote pushed at the end. The job of the conversation is to find out, honestly, whether we should be working together.

Get in touch

Phone: 1300 859 910
Web: agileit.com.au
Email: admin@agileit.com.au
Mornington: Building C 6/41 Watt Rd, Mornington VIC 3931
Melbourne: Level 2/88 Jolimont St, East Melbourne VIC 3002