FREE CHECKLIST NDIS IT Security

NDIS Provider IT Security Checklist

8 areas every NDIS organisation must address — Essential Eight, Privacy Act & NDIS Practice Standards

Fixable | 0435 955 429 | fixable.au | NDIS Worker Screening Cleared

Every 6 min	$46,000	19%
Cybercrime occurs in Australia (ACSC)	Avg SMB cybercrime cost in Australia	Of all breaches: health & disability

Legal obligations apply to ALL NDIS providers: Privacy Act 1988 (updated 2025 — small business exemption removed), Cyber Security Act 2024, Notifiable Data Breaches scheme (30-day reporting), and NDIS Practice Standards Information Management module (audited).

1 ■ Passwords & MFA

HIGHEST PRIORITY

- [ ] **MFA enabled on email, case management & PRODA/myID** — HIGH
  Two-step login — stolen passwords can't get in without your phone
- [ ] **No shared login credentials** — HIGH
  Each staff member has their own unique username and password
- [ ] **Passwords 14+ characters or password manager in use**
  Bitwarden or 1Password — free options available
- [ ] **Admin accounts separate from day-to-day accounts**
  Admin rights restricted to those who genuinely need them
- [ ] **Departed staff accounts disabled immediately** — HIGH
  Documented IT offboarding process in place

2 ■ Software Updates

Patch critical vulns within 48 hrs

- [ ] **Windows / macOS fully up to date on all devices** — HIGH
  Auto-updates enabled — do not click "Remind me later"
- [ ] **Microsoft Office / Google Workspace is current version**
  No staff using Office 2013 or other end-of-life software
- [ ] **No devices running Windows 10 after October 2025** — MED
  Windows 10 end-of-life Oct 2025 — upgrade to Windows 11
- [ ] **Web browsers on current version**
  Chrome, Edge, Firefox — auto-updates enabled

3 ■■ Data Encryption & Storage

Privacy Act APP 11

- [ ] **Participant records in encrypted, cloud-based system** — HIGH
  NOT on local hard drives, USBs, or personal Google Drive
- [ ] **Data stored in Australian data centres**
  NDIA requires participant data cannot be stored or accessed offshore
- [ ] **Laptop hard drives encrypted**
  BitLocker (Windows) or FileVault (Mac) on all portable devices
- [ ] **No sensitive data shared via personal email or SMS**
  Documented policy for how participant info is shared between staff

4 ■ Backups

Your last line of defence

- [ ] **Automated daily backups running** — HIGH
  Not manual. Not weekly. Not "when I remember."
- [ ] **Backup stored separately from main system**
  Separate cloud account or offline — ransomware cannot encrypt it
- [ ] **Backup restore tested in last 6 months** — HIGH
  Most providers discover their backup fails only when they need it
- [ ] **90+ day backup retention**
  Ransomware can lie dormant — you need older restore points

5 ■ Email Security

91% of breaches start with phishing

- [ ] **Staff trained to recognise phishing emails** — HIGH
  Know what suspicious emails look like and who to report them to
- [ ] **Business email uses a custom domain**
  Not free Gmail/Hotmail for official NDIS communications
- [ ] **Spam filtering and email scanning active**
  Microsoft 365 Defender or Google Workspace protection enabled
- [ ] **Process exists for reporting suspicious emails**
  Staff know exactly what to do when they get a suspicious email

6 ■■ Role-Based Access Control

Checked during NDIS audits

- [ ] **Staff access only records relevant to their role** — HIGH
  Support worker ≠ financial records. Admin ≠ clinical notes.
- [ ] **Access reviewed when roles change**
  Promotions, moves, and departures trigger immediate access review
- [ ] **Audit trail exists in case management software**
  Log of who accessed which records — required by NDIS auditors

7 ■ Device Security

SIL tablets & remote workers

- [ ] **All work devices have antivirus / endpoint protection**
  Microsoft Defender (free, built into Windows 11) is a good start
- [ ] **Devices auto-lock after 5–10 minutes of inactivity**
  Critical for SIL house tablets that may be left unattended
- [ ] **Clear BYOD policy if personal devices are used for work**
  Staff personal devices touching participant data need rules
- [ ] **Lost/stolen devices can be remotely wiped** — HIGH
  Essential for field staff tablets with participant data

8 ■ Incident Response & Breach Reporting

30-day NDB reporting requirement

- [ ] **Written incident response plan exists** — HIGH
  Staff know who to call, what to shut down, who is responsible
- [ ] **Staff understand notifiable breach obligations**
  Unauthorised access causing serious harm = report to OAIC within 30 days
- [ ] **Incident log maintained**
  Security incidents recorded and reviewed — required by NDIS auditors
- [ ] **Ransomware payment reporting understood**
  Cyber Security Act 2024: payments must be reported to govt within 72 hrs

Score your organisation

Score	Risk level	What to do
0–12 ticks	High risk	Act immediately — call Fixable for a free assessment
13–22 ticks	Moderate risk	Prioritise MFA, backups, and access control first
23–28 ticks	Good foundation	Maintain documentation and review annually

Free on-site IT security assessment for NDIS providers

Call 0435 955 429 | fixable.au

Melbourne eastern & south-eastern suburbs • NDIS Worker Screening cleared • No jargon, no upselling