

NDIS IT Audit-Readiness Checklist

25 checks an owner or operations manager can run in an afternoon. They cover the technology side of what auditors look for under the NDIS Practice Standards, and what the Privacy Act expects of anyone holding participant health information.

How to use it: tick a box only if the answer is "yes, and I could show evidence today". A "we think so" is a no. Then count your ticks and check your score on the last page.

1. Who can get in

Practice Standards: Information Management · Human Resource Management

- 1 ☐ **Every person who has left has had their accounts disabled.**
Compare active email, rostering and case-note accounts against your current staff list.
- 2 ☐ **Access is removed on a worker's last day, by a named person, using a written checklist.**
- 3 ☐ **Every staff account needs a second step to log in (multi-factor login).**
Check email first, then your care platform.
- 4 ☐ **Nobody shares a login.**
Shared "admin@" or "house1@" logins mean you can't show who viewed a participant's record.
- 5 ☐ **No more than two or three people have full administrator rights, and you can name them.**
- 6 ☐ **Workers can see only the participants they support.**
Roles in your care platform match what each person needs.

2. Email and files

Practice Standards: Information Management · Risk Management

- 7 ☐ **No participant files are shared with "anyone with the link".**
Check the sharing report in Microsoft 365 or Google Drive.
- 8 ☐ **Participant information is stored in business systems, not personal email, WhatsApp or personal cloud drives.**
- 9 ☐ **Your email domain has SPF, DKIM and DMARC set up.**
These stop criminals sending email that looks like it came from you.
- 10 ☐ **Old sign-in methods that skip multi-factor login are blocked.**
- 11 ☐ **Sign-in and file-access logs are switched on and kept.**
You'll need them to work out what happened after an incident.

3. Laptops and phones

Practice Standards: Information Management · Risk Management

- 12 ☐ **Every laptop is encrypted.**
BitLocker on Windows, FileVault on Mac.
- 13 ☐ **Every phone that opens participant information has a passcode and can be wiped remotely.**
This includes workers' personal phones.
- 14 ☐ **Devices install updates automatically.**
- 15 ☐ **Staff know who to call, the same day, if a device is lost or stolen.**
- 16 ☐ **You keep a list of the devices that can access participant information.**

4. Backup and keeping supports running

Practice Standards: Continuity of Supports · Emergency and Disaster Management

- 17 ☐ **Email and files are backed up somewhere other than Microsoft or Google.**
Their built-in recycle bins are not a backup.
- 18 ☐ **You have restored something from backup in the last 12 months, and recorded the date.**
- 19 ☐ **You know how to export your data from your care platform.**
- 20 ☐ **There is a written plan for delivering supports if rosters or notes are offline for a day.**

5. Privacy and incidents

Practice Standards: Privacy and Dignity · Incident Management · Privacy Act 1988 (Notifiable Data Breaches scheme)

- 21 ☐ **You have a written data breach response plan that names who decides and who notifies.**
- 22 ☐ **Staff have had privacy and phishing training in the last 12 months, with a record of who attended.**
- 23 ☐ **Your privacy policy matches where participant information is really stored.**
- 24 ☐ **You keep a list of every app that holds participant information, with an owner for each.**

6. Software spend

Good governance: money back into supports

- 25 ☐ **In the last 12 months someone compared licences paid for against licences in use, and cancelled the difference.**

21–25 ticks

Strong. Keep the evidence (screenshots and dates) together for your auditor.

13–20 ticks

Gaps an auditor is likely to ask about. Fix checks 1, 3, 7 and 21 first.

12 or fewer

Participant information is likely exposed now. Start with checks 1 and 3 this week.

Want this checked independently? Our 5-day Tech Health Check verifies these controls in your systems, maps the gaps to the Practice Standards and finds the software spend you can cut. Fixed price, and free if we find neither savings nor a material gap. Book a 15-minute call at 5foldstrategy.com/ndis.

This checklist is general guidance, not legal advice and not an NDIS audit. Only an NDIS Commission approved quality auditor can assess conformity with the NDIS Practice Standards. Fivefold AI is independent and is not affiliated with the NDIA or the NDIS Quality and Safeguards Commission. © 2026 Fivefold AI.