

This is a sample report. "Example Community Supports" is a fictional provider and every figure is illustrative. It shows the format and level of detail you receive, not a real client's results.

Tech Health Check Report

Example Community Supports (fictional) · Report v1.0

Prepared for	Chief Executive Officer and Operations Manager
Organisation	Registered NDIS provider · SIL and community participation · 42 staff · 3 sites · next audit in 4 months
Systems reviewed	Microsoft 365 · care platform (rostering and case notes) · accounting · 14 other subscriptions
Prepared by	Jayden Le, CISSP · Fivefold AI

Executive summary

Overall rating: **Red**. Participant information is exposed today in four places, and all four can be fixed in about 10 hours of work. We also found \$7,752 a year in software savings.

4

red findings, fix within 7 days

10

amber findings, fix within 30 days

\$7,752

a year in software savings found

The three things to fix first

- Former workers can still log in.** 11 people who have left still have active accounts with access to email and the care platform. The oldest left 7 months ago.
- One in four staff can log in with only a password.** A single phished password would open participant case notes.
- Email and files have no backup outside Microsoft.** A ransomware attack or a mistaken bulk delete could not be reversed after 93 days.

Scorecard

AREA	RATING	HEADLINE FINDING
1. Identity & access	Red	11 former workers active; multi-factor login on 74% of staff
2. Microsoft 365 security	Red	23 files shared with "anyone with the link"
3. Devices	Amber	2 of 8 sampled laptops not encrypted
4. Backup & recovery	Red	No independent backup; no restore test on record
5. Privacy & breach readiness	Amber	No written data breach response plan
6. Software & SaaS spend	Amber	\$7,752 a year in savings across 4 subscriptions

Evidence labels used in this report: **Verified** = we checked the setting or record directly. **Sampled** = we checked a sample. **Reported** = based on what your team told us.

Detailed findings

1. Identity & access

Practice Standards: Information Management · Human Resource Management · Risk Management

FINDING	RATING	EVIDENCE	FIX
11 of 53 active accounts belong to people no longer on the staff list	Red	Verified	Disable today. Adopt an offboarding checklist owned by the Operations Manager.
Multi-factor login enforced for 31 of 42 staff (74%)	Red	Verified	Enforce for all users with a Conditional Access policy.
5 people hold global administrator rights	Amber	Verified	Reduce to 2 named admins using separate admin accounts.
Shared "roster@" login used by 6 coordinators	Amber	Reported	Replace with a shared mailbox and individual logins.
All 7 coordinators have full administrator role in the care platform	Amber	Sampled	Move 5 coordinators to the coordinator role.

2. Microsoft 365 security

Practice Standards: Information Management · Risk Management

FINDING	RATING	EVIDENCE	FIX
23 files and 4 folders shared with "anyone with the link". Folder names suggest participant documents.	Red	Verified	Remove public links. Limit sharing to named people.
Legacy sign-in methods that bypass multi-factor login are not blocked	Amber	Verified	Block legacy authentication.
No DMARC record on the email domain	Amber	Verified	Publish DMARC in monitor mode, then enforce.
Audit logging is switched on	Green	Verified	No action. Keep as audit evidence.

3. Devices

Practice Standards: Information Management · Risk Management

FINDING	RATING	EVIDENCE	FIX
6 of 8 sampled laptops are encrypted	Amber	Sampled	Turn on BitLocker for all laptops and record it.
Support workers use personal phones with no enforced passcode or remote wipe	Amber	Reported	Apply an app protection policy to work apps on personal phones.
Sampled devices install updates automatically	Green	Sampled	No action.

4. Backup & recovery

Practice Standards: Continuity of Supports · Information Management

FINDING	RATING	EVIDENCE	FIX
Email, OneDrive and SharePoint have no backup outside Microsoft 365	Red	Verified	Add a third-party Microsoft 365 backup. About \$4 a user a month.
No record of a restore test	Amber	Reported	Test a restore once the backup is in place. Record the date.
Care platform data export process is documented	Green	Reported	No action.

5. Privacy & breach readiness

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

FINDING	RATING	EVIDENCE	FIX
No written data breach response plan	Amber	Reported	Adopt a 2-page plan naming who assesses, decides and notifies.
Last privacy and phishing training was more than 2 years ago; no attendance record	Amber	Reported	Run a 30-minute session and keep the attendance list.

Software & SaaS savings

We found **\$7,752 a year** in savings across 4 subscriptions. That is 12.6% of current software spend of \$61,400 a year.

SUBSCRIPTION	ISSUE	ACTION	SAVING / YR
Microsoft 365 Business Premium	9 licences assigned to former workers or unused for 90+ days	Remove 9 licences	\$3,564
Video meeting tool	12 paid seats; Microsoft Teams is already included	Cancel at renewal	\$2,640
Online forms tool	Duplicates forms built into the care platform	Cancel	\$948
E-signature tool	On a higher plan than the features used	Downgrade one tier	\$600
Total			\$7,752

Savings are estimates from prices and usage at the time of review. Your report also includes the full inventory of every subscription, its owner, renewal date and whether it holds participant information.

30-day fix plan

#	ACTION	FIX BY	WHO	EFFORT
1	Disable the 11 former-worker accounts	Within 7 days	Client	1 hr
2	Enforce multi-factor login for all staff	Within 7 days	Fivefold AI or IT provider	3 hrs
3	Remove public sharing links on files and folders	Within 7 days	Client	2 hrs
4	Set up Microsoft 365 backup and test a restore	Within 7 days	Fivefold AI or IT provider	4 hrs
5	Cut admin rights; fix care platform roles; replace shared login	Within 30 days	Client	3 hrs
6	Encrypt laptops; protect work apps on personal phones	Within 30 days	Fivefold AI or IT provider	6 hrs
7	Adopt breach response plan; run staff training	Within 30 days	Client	4 hrs
8	Block legacy sign-in; publish DMARC	Within 30 days	Fivefold AI or IT provider	2 hrs
9	Cancel or downgrade the 4 subscriptions	Within 30 days	Client	2 hrs

Scope and limitations

This review used read-only access and covered the systems listed on page 1. Findings reflect settings at the time of review. It is not an NDIS registration audit, penetration test or legal advice. Only an NDIS Commission approved quality auditor can assess conformity with the NDIS Practice Standards.

Want this for your organisation? The Tech Health Check is \$1,490 ex GST (launch price), delivered in 5 business days, and free if we find neither savings nor a material gap. Book a 15-minute call at 5foldstrategy.com/ndis.

Sample report. Fictional organisation and illustrative figures. Fivefold AI is independent and is not affiliated with the NDIA or the NDIS Quality and Safeguards Commission. © 2026 Fivefold AI.