



Backup & Recovery Policy

What we back up, where, and how we know it works.

Backups are what turn a ransomware attack or a lost device from a disaster into an inconvenience. This policy sets out how [Business name] protects its data.

Rules

Deputy owner(s): _____

- **What & when.** Business files, and our Microsoft 365 / Google Workspace data, are backed up automatically every day.
- **3-2-1.** We keep at least three copies, on two types of media, with one copy offline or isolated so ransomware can't reach it (the 3-2-1 rule).
- **Test it.** We test a real restore at least quarterly and record how long it took.
- **Ownership.** A named person is responsible, and at least one other person knows how to access the backups.

Backup owner: _____

What's backed up: _____

Last restore test (date): _____

Make it yours (with AI)

I run a [type of business] in [town], Australia, with [number] staff. Rewrite the policy below so it fits how my business actually works, in plain English my team will read. Keep it to one page. [paste the template]

Two rules: start a fresh chat, and never paste real customer names, bank details or staff records into a free AI tool.