07. Backup and recovery policy

> **Template.** Part of the open-source AI App Policy Kit, version 1.0. Replace everything in [square brackets], delete what does not apply, and have the person who runs the business approve it. A starting point, not legal advice.

Business	[Business name]
Document owner	[Name and role]
Approved by, and date	[Name], [date]
Next review	[Date, at most 12 months on]

Why this matters

A backup you have never restored is a hope, not a plan. Apps built quickly often run on one database with whatever backup the platform switched on by default, and nobody has checked that it can be brought back.

Who it covers

Every system that holds data [Business name] could not easily recreate: the app's database, uploaded files, source code, configuration, and the documents and email the business runs on.

The rules

1. **List what must be backed up** in the table below, with how much you can afford to lose and how long you can be without it.
2. **Back up automatically.** Daily at least for the database. Nobody has to remember.
3. **Keep three copies, in two places, one of them elsewhere.** The live data, a backup with the same provider, and a copy in a different account or with a different provider.
4. **Protect backups from deletion.** At least one copy cannot be changed or deleted by the app's own login, or by a single person, for [30] days. This is the copy that survives ransomware and mistakes.
5. **Encrypt backups** and limit who can read them. A backup holds everything the database holds.
6. **Test a restore every [3 or 6] months.** Restore to a separate place, check the data opens and is complete, and record how long it took.
7. **Keep backups only as long as needed.** Backups hold personal data, so their life is part of the retention schedule (document 10).
8. **Code and configuration are backed up too.** The source code is on a code host, and the set-up of the cloud account is written down or kept as code, so the app can be rebuilt from nothing.
9. **Write the recovery steps down** where they can be read when the systems are down.

What is backed up

System	How often	Where the copies are	Protected from deletion?	Most data we can lose	Longest time down	Kept for
App database	[Daily, plus point-in-time]	[Provider; second account]	[Yes, 30 days]	[1 hour]	[4 hours]	[35 days]
Uploaded files	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Source code	[Every change]	[Code host; mirror]	[ ]	[None]	[1 day]	[ ]
Documents and email	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Restore test log

Date	System	Restored by	Time taken	Data complete?	Problems found and fixed
[Date]	[App database]	[Name]	[40 minutes]	[Yes]	[ ]

Recovery steps

1. [Who decides to restore, and how to reach them.]
2. [Where the backups are and which login opens them.]
3. [The steps to restore the database to a new instance.]
4. [How to point the app at the restored data.]
5. [How to check the app works, and who tells customers.]

Checklist

- ☐ Every system in the table has an automatic backup.
- ☐ One copy is in a different account or with a different provider.
- ☐ One copy cannot be deleted by the app or by one person alone.
- ☐ A restore was tested on schedule and the time taken is within "longest time down".
- ☐ The recovery steps were followed by someone other than their author.

References

- NCSC, *Small Business Guide: Backing up your data* and *Offline backups in an online world*.

AI App Policy Kit, version 1.0. © 2026 PugliseWeb LTD, licensed under CC BY 4.0: use it, change it and share it, with credit. The whole kit, and a free Software Health Check of your app against it: https://www.puglieseweb.com/ai-policy-kit