The 3-2-1 Rule

3 copies	**of your data**
2 different	**storage types**
1 offsite	**location**

This isn't paranoia — it's math. Hard drives fail. Cloud providers have outages. Ransomware encrypts everything it can reach. The 3-2-1 rule ensures no single failure mode can take you down.

What this looks like in practice

- **Copy 1:** Your working files (local machine)
- **Copy 2:** External drive or NAS (different device)
- **Copy 3:** Cloud backup or offsite drive (different location)

Version Control Everything

If it's text, it belongs in Git. Code, configuration, documentation, scripts — all of it. Version control gives you:

- Complete history of every change
- Ability to roll back mistakes
- Built-in offsite backup (GitHub, GitLab, etc.)
- Collaboration without chaos

Don't limit this to code. Infrastructure as code, dotfiles, even notes — if it matters, version it.

Practice Restores

A backup you've never tested is not a backup. It's a hope.

Schedule regular restore drills. Quarterly at minimum. Actually restore files. Spin up from your backups. Time how long it takes. Find the gaps before an emergency finds them for you.

Restore drill checklist

- Can you actually access your backups?
- Do you have the passwords/keys needed?
- How long does a full restore take?
- Is the restored data complete and usable?
- Who else knows how to do this if you're unavailable?

← ALL PLAYBOOKS