Sentrly — Cloud Backup Checklist

What to back up, where, and how to verify restoration actually works.

People

- ■ Document who owns security decisions today (even if it's the founder).
  Without a named owner, security is everyone's problem and no one's job.
- ■ Run a 30-minute phishing-and-passwords briefing for everyone.
  Most incidents start with an email or a reused password. Start there.
- ■ Define a simple offboarding checklist: revoke email, SSO, repos, admin tools, key cards.
  Forgotten access is a leading cause of insider-style incidents.

Accounts & access

- ■ Adopt single sign-on (SSO) for as many tools as your stack allows.
  One identity provider means one place to disable a leaver's access.
- ■ Require phishing-resistant 2FA (TOTP or hardware keys) for all admins.
  Admin compromise is the worst-case scenario. Make it expensive.
- ■ Use a shared password manager for credentials that can't go through SSO.
  Email + spreadsheet is not a strategy; a manager gives audit and revocation.
- ■ Apply least-privilege roles in cloud, source control and finance tools.
  Default 'admin for everyone' is the most common high-impact misconfiguration.

Devices

- ■ Require disk encryption on every laptop. Verify quarterly.
  Stolen laptops with unencrypted disks are an instant breach for any business with customer data.
- ■ Enroll laptops in a basic MDM or device-management tool.
  Even a free tier lets you enforce a screen-lock, push updates, and wipe a lost device.
- ■ Set automatic OS and browser updates. Verify on a sample monthly.
  'We update sometimes' is not a defense — verify.

Data & vendors

- ■ Inventory the SaaS apps you pay for. Note what data each holds.
  You can't protect what you can't list. The list rarely grows shorter on its own.
- ■ Pick one canonical place for sensitive customer data; don't let it sprawl.
  Sprawl makes legal-hold, deletion-on-request and incident-response far harder.
- ■ Configure backups for production data with at least one off-site copy.
  Ransomware is a business-continuity issue, not a security-team-only issue.

Incident response

■ Write a one-page playbook: who to call, where to find logs, who can speak to customers.
Decisions made calmly in advance beat decisions made at 2am.

■ Have a way to reach every employee out-of-band (e.g. SMS list) in case email is down.
If the incident is in your email tenant, in-tenant comms aren't trustworthy.

■ Know your breach-notification obligations for your jurisdictions and customer contracts.
Timelines are short — don't research them while a clock is running.