RECOVERY

Test a Backup by Trying to Work with It

The dashboard shows a green tick every night. When a folder needs restoring, it contains documents but not the attachments that made them useful. The backup ran successfully. The work still cannot continue.

Choose Something a Person Needs to Use

A useful test begins with a specific task, such as opening an order record and finding its documents. Agree with the person who does that work what should be present, from which date and with which permissions. Restore a sample in a separate environment without overwriting current data.

Measure the time from the recovery request until that person can use the restored material. Include finding the backup, getting approval and obtaining the necessary keys. Download time is only part of the process.

What to Record

- The date of the recovered data and the later work that would need reconstructing.
- Any missing files, settings or attachments.
- Who can restore the data and what happens when that person is unavailable.
- Whether the credentials that can delete the originals can also delete every backup.

Review synchronisation separately. Depending on its configuration, it may carry a deletion across devices. Check versions, retention and recovery instead of assuming that every synchronised folder is an independent backup. Agree protection for important data that does not depend on the same point of failure.

Repeat the test when an application or storage process changes. Keep the results with their limits: recovering a sample establishes that the sample worked, not that an entire system could return within the same time.

> *Recovery time and completeness depend on the available backups and the incident. A bounded test provides evidence, not a guarantee of total recovery.*

A Check You Can Run

A small exercise could restore a sample order and its attachment into an isolated environment. Have the person who normally processes orders confirm that both open and can be used together. Record the backup’s age and the time spent restoring and checking it. Keep production untouched; a successful file copy alone does not establish that the business can resume work.

Supporting guidance: CISA’s guidance on backup testing and recovery.
https://www.cisa.gov/stopransomware/ransomware-guide

Continue with: The Old Website Nobody Remembers May Still Be Online.
https://systems.kavaliero.com/en/blog/the-old-website-nobody-remembers-may-still-be-online

For help with this work, see the scope of Security Audits & Penetration Testing.
https://systems.kavaliero.com/en/services/security-audits