

WEBSITE BACKUP & RECOVERY CHECKLIST

A practical guide for small businesses · Independent, vendor-neutral IT Club guidance

CLOUD HOSTING IS NOT THE SAME AS AN INDEPENDENT BACKUP

A code copy is a useful start. A recoverable website may also need data, files, secrets, DNS, domain access, deployment settings and a tested route back to a working site.

LIVE WEBSITE > INDEPENDENT COPIES > TESTED RECOVERY

1 PROTECT THE COMPONENTS

- ☐ Source code copied outside the primary platform
- ☐ Commit history and useful previous versions retained
- ☐ Database backup and retention understood
- ☐ Uploads, media and generated documents protected
- ☐ DNS records documented or exportable
- ☐ Domain registrar under business control

2 PROTECT ACCESS

- ☐ Secrets and API credentials stored securely
- ☐ No production secrets committed to Git
- ☐ Hosting and deployment access documented
- ☐ More than one appropriate person can recover access
- ☐ GitHub, hosting and registrar accounts use MFA

3 REPLIT + GITHUB EXAMPLE

- ☐ Create an empty private GitHub repository
- ☐ Understand the existing Replit Git setup
- ☐ Add GitHub as an additional remote
- ☐ Push the intended branch and verify history
- ☐ Repeat after meaningful batches of work

4 KNOW THE DEPENDENCIES

- ☐ Forms and email delivery listed
- ☐ Third-party integrations and webhooks listed
- ☐ Deployment settings can be recreated
- ☐ Database, storage and external services have owners
- ☐ Recovery notes name the rebuild dependencies

SAFE EXAMPLE COMMANDS

```
git remote -v
git remote add github https://github.com/USERNAME/REPOSITORY.git
git status
git push -u github main
```

Understand the current project and remote configuration before running Git commands.

RECOVERY IS THE TEST

Website Backup & Recovery Checklist · A backup that has never been restored is an assumption

RPO = HOW MUCH RECENT WORK COULD YOU LOSE?

RTO = HOW LONG COULD THE WEBSITE BE UNAVAILABLE?

5 FREQUENCY + RETENTION

- ☐ Backup frequency follows how much can be lost
- ☐ Static site schedule is proportionate
- ☐ Frequently edited site has more frequent protection
- ☐ Transactional data has an agreed recovery point
- ☐ Old versions are retained for a known period

6 RESTORE TEST

- ☐ Someone owns the restore decision
- ☐ An authorised person can access every component
- ☐ Restore is tested away from the live site
- ☐ Database and uploads are included in the test
- ☐ The restored site is actually checked
- ☐ Failed steps become recovery-note actions

RECOVERY QUESTIONS

1. Who owns the backup and the recovery decision?
2. Who can access the repository, data, storage, domain and hosting?
3. Is the backup independent from the live hosting platform?
4. What happens if the hosting supplier disappears or the account is locked?
5. Could another authorised developer restore the site?
6. When did anyone last prove that the backup works?

RED FLAG

If the only copy of the site, its data and its backup all depend on the same account or supplier, you may still have a single point of failure.

DO THIS THIS WEEK

Write down the hosting platform, registrar, DNS provider, source-code location, database location and current backup method. Then ask what you could actually recover if the primary platform vanished.

IT CLUB TAKEAWAY

Know what you own, what is protected and how you get it back. This checklist is practical guidance, not a backup service, certification or guarantee of recovery.