dacros

A FREE DACROS CARD

The backup and restore checklist

A backup is a copy you have restored at least once. This card sets out the copies we recommend: encrypted before they leave the business, kept with a second provider in the UK or the EU, protected from deletion, and proved by restoring them.

EDITION
Edition 1 · November 2026

FOR
Any business that has backups, or thinks it has

ONLINE
dacros.com/resources/backup-and-restore-checklist

What to back up

- [ ] **All the data the business needs to operate:** email, documents, invoicing, contacts, customer records and the website [1].
- [ ] **What a restore needs besides the data:** settings, licence details, the list of accounts and how each is recovered, and the backup's own encryption key, kept apart from the backup.
- [ ] **Every new system,** added to the backup the week it starts holding data.

How the copies are kept

- [ ] **More than one copy, in more than one place.** The NCSC suggests both an online backup and a storage device, in case one is lost, stolen or fails [1].
- [ ] **Encrypted before it leaves the business,** with a key you hold and the backup provider does not. The provider then stores data it cannot read. UK GDPR names encryption among the measures for keeping personal data secure [3].
- [ ] **With a second provider,** not the one that runs the system it protects, so a lockout or a deleted account cannot take the system and its backup together.
- [ ] **In the UK or the EEA.** Copies kept in the UK stay inside the UK, and every EEA country has full UK adequacy, so neither needs a transfer safeguard for the copies [4].
- [ ] **Protected from deletion:** versions that cannot be changed or deleted for a period you set, or deletions that can be undone, so an attacker who gets in cannot destroy the backups [2].
- [ ] **Behind a separate sign-in,** with two-step verification, not shared with the everyday administrator accounts [1, 2].
- [ ] **A storage device unplugged** when it is not in use: some viruses also reach devices connected to an infected computer [1].
- [ ] **Alerts** when a backup fails, and when someone tries to delete or change backups or their settings [2].

The restore test

- [ ] Restore one folder and one person's email to a different place, open them, and check they hold what you expected [1].
- [ ] Restore from an older version too, not only the latest, in case the latest copy is already damaged [2].
- [ ] Once a year, restore a whole system and time it, from start to working: that time is your real recovery time.
- [ ] Check you could reach the backup, and its key, if the office, your main email and your own laptop were all out of action [2].
- [ ] Write down each test: the date, what was restored, how long it took and what went wrong. UK GDPR asks for the ability to restore personal data in a timely manner, and for a process for regularly testing your security measures [3].

TEST DATE	WHAT WAS RESTORED	HOW LONG IT TOOK	WHAT WENT WRONG, AND THE FIX

Every month

- [ ] Read the backup reports, and look into any failure or warning.
- [ ] Check that the newest backup is from when you expect.
- [ ] Check that the people who can sign in to the backup are still the right people.

Sources

[1] NCSC, Small organisations guide to cyber security: backing up your data, published 9 April 2026, reviewed 21 July 2026, checked 10 November 2026 · ncsc.gov.uk

[2] NCSC, Principles for ransomware-resistant cloud backups, published 22 November 2024, checked 10 November 2026 · ncsc.gov.uk/guidance/principles-for-ransomware-resistant-cloud-backups

[3] UK GDPR, Article 32, Security of processing, paragraph 1, checked 10 November 2026 · legislation.gov.uk/eur/2016/679/article/32

[4] ICO, Is the restricted transfer covered by adequacy regulations?, checked 10 November 2026 · ico.org.uk