CORE NETWORK SOLUTIONS

Backup and recovery checklist

Will your backups be there when you need them?

Backups only matter on the day you need them. Use this checklist to make sure you can get your data back after a failure, a mistake or a ransomware attack.

What's covered

- [ ] We know which systems and data are backed up, and which aren't.
- [ ] Servers, virtual machines and file shares are backed up.
- [ ] Microsoft 365 email, OneDrive, SharePoint and Teams are backed up separately.
- [ ] Line-of-business applications and their databases are backed up properly, not just copied.

The 3-2-1 rule

- [ ] We keep at least three copies of important data.
- [ ] Backups are on at least two different kinds of storage.
- [ ] At least one copy is off site.
- [ ] At least one copy can't be changed or deleted for a set time (immutable), or is offline.

Recovery goals

- [ ] We've agreed how much data we could afford to lose (recovery point objective).
- [ ] We've agreed how quickly each system must be back (recovery time objective).
- [ ] Our backup schedule and recovery method meet those goals.

Checks and tests

- [ ] Someone checks every day that backups completed, and fixes failures.
- [ ] We test restoring a file, a mailbox and a whole system at least a few times a year.
- [ ] We've timed a full recovery, and it meets our recovery goals.

Security

- [ ] Backups are encrypted in transit and at rest.
- [ ] Backup systems use separate credentials, with multi-factor authentication.
- [ ] We know where our backups are stored, including which country.

> **Next step**
>
> If you can’t tick every box, you’re not alone. We can review your backups and help you build a recovery plan you can rely on.