

Backup & Disaster Recovery Checklist

Having backups isn't the same as being able to recover. This checklist walks through what you're protecting, how it's backed up, whether anyone is watching, and whether you've proven a restore works.

How to use: Check only what you can confirm is in place today, then total your checks at the end.

1 Know what matters

___ / 4

- ☐ **You have a list of critical systems and where each one's data lives**
Servers, cloud apps, Microsoft 365, line-of-business software, and key laptops.
- ☐ **You've decided how long you can afford to be down (RTO)**
In business terms: hours, a day, a week?
- ☐ **You've decided how much data you can afford to lose (RPO)**
The last hour of work? The last day?
- ☐ **Cloud data is included in the plan**
Microsoft 365 and SaaS apps need their own backup.

2 Backup design

___ / 6

- ☐ **Backups follow the 3-2-1 rule**
Three copies, on two types of storage, with one copy offsite.
- ☐ **At least one copy is immutable or off line**
Ransomware routinely targets backups first.
- ☐ **Backups run automatically, at least daily**
No one has to remember to plug in a drive.
- ☐ **Backups are encrypted**
In transit and at rest.
- ☐ **Retention is long enough to recover from an attack found weeks later**
Attackers often sit quietly before striking.
- ☐ **Backup system logs are separate from your everyday network accounts and use MFA**
A compromised admin account shouldn't be able to delete your backups.

3 Monitoring

___ / 2

- ☐ **Someone checks backup results every day**
Or an automated alert goes to someone who responds.

- ☐ Failed or skipped backups are fixed within one business day
And the cause is noted.

4 Testing

___ / 3

- ☐ A file-level restore is tested at least quarterly
Pick random files and confirm they open.
- ☐ A full system recovery is tested at least annually
Time it. Does it meet your RTO?
- ☐ Test results are documented
What was restored, how long it took, and any problems.

5 Continuity plan

___ / 4

- ☐ A written disaster recovery plan exists
Step-by-step, not in someone's head.
- ☐ The plan is stored where you can reach it if systems are down
Printed copy or a separate cloud location.
- ☐ You know how staff will work if the office or internet is unavailable
Cloud access, failover internet, laptops at home.
- ☐ An up-to-date contact list includes staff, vendors, IT support, and your insurer

Your score

Items checked: _____ of 19 = _____ %

90-100%

Strong

You have solid fundamentals.
Review this checklist twice a year
to keep it that way.

65-89%

Gaps to close

A good base with a few real
exposures. Start with the
unchecked items in the first two
sections.

Below 65%

At risk

Several core protections are
missing. Prioritize now, before an
incident sets the agenda for you.

Find out if your backups would really work.

FUSION 1 can run a restore test with you and show you exactly how long recovery would take.

[Book a free IT review](#)

Call or text 814-499-2119
Toll-free 888-279-9776

This checklist is general guidance for small businesses and is not legal, compliance, or insurance advice. © 2026 FUSION 1 IT Solutions. You're welcome to share this document unchanged.