

IT Disaster Recovery Checklist for Businesses



Your Business Recovery Checklist

When something goes wrong with your technology, whether it's a cyber attack, a failed server or a flood, the businesses that recover quickly are the ones that planned before it happened. Every hour offline costs you sales, wages and customer confidence.

This checklist covers the essentials of IT disaster recovery in plain English. Tick off what you already have, and note what you don't. Every unticked box is a risk worth knowing about.

Get Ready

01

Name an owner: A senior person is responsible for disaster recovery, with a named deputy to cover holidays and sickness.

☐

02

Have a written plan: Your plan is written down and approved by a director. Short and clear beats long and unread.

☐

03

List what you've got: Keep an up-to-date list of every computer, server, app and cloud service, and who looks after each

☐

04

Know what matters most: Agree which systems you couldn't work without, so you know exactly what to restore first.

☐

05

Set recovery targets: Agree how long each system can be down, and how much recent work you could afford to lose.

☐

06

Write down phone numbers: Out-of-hours numbers for your team, suppliers and IT provider, kept somewhere you can reach without your systems.

☐

Protect your Backups

07

Automatic backups: Your important data is backed up automatically, so it never relies on someone remembering

☐

08

Keep a copy off-site: At least one copy is stored away from your office, for example in the cloud.

☐

09

Keep an untouchable copy: At least one copy can't be changed or deleted by an attacker (offline or "immutable").

☐

10

Back up Microsoft 365 or Google: These services keep running, but they don't protect you from every deletion, hacked account or late-spotted mistake.

☐

11

Encrypt your backups: Make sure backed-up data is encrypted so it's useless to anyone who shouldn't see it.

☐

12

Act on backup alerts: Someone reads the backup alerts every day and acts when something fails.

☐

13

Test restoring files: Restore a few files from backup at least every three months to prove it really works.

☐

14

Lock down admin accounts: Switch on multi-factor authentication for admin accounts and backup tools.

☐

Get Back Up and Running

15

Know your recovery order: You've agreed which systems come back first, second and third.

☐

16

Write step-by-step instructions: Simple instructions exist for your most important systems, clear enough for someone who didn't write them.

☐

17

Have a backup internet connection: Even a 4G or 5G router can keep your business going while your main line is down.

☐

18

Store licence keys and admin logins safely: Keep them secure but reachable in an emergency, not only on the system that's failed.

☐

19

Keep supplier contracts current: Support contracts are in date and their contact details are written down.

☐

Look After your People

20

Make sure staff know what to do: Everyone knows who to call and what to do if systems go down.

☐

21

Have a back-up way to reach everyone: A WhatsApp group, text service or phone tree for when email and Teams are down.

☐

22

Prepare your messages: Draft messages for staff and customers are ready to go, so you're not writing them under pressure.

☐

23

Know your data breach duties: You know who decides whether to report a breach to the ICO, and how. The clock is 72 hours.

☐

24

Record your cyber insurance details: Your policy details and claims number are written down where you can find them.

☐

Practice and Review

25

Talk through a “what if”: In the last six months, you've sat down as a team and walked through a scenario like ransomware.

☐

26

Run a full restore test: In the last twelve months, you've restored a whole system from backup, not just a few files.

☐

27

Update after changes: The plan was reviewed after your last big system change, office move or incident.

☐

28

Keep an offline copy of the plan: A printed or offline copy is stored somewhere safe, so you can read it when your systems are down.

☐

How did you do?

0 to 11 ticked: There are some real gaps, but this is very fixable. Start with an off-site backup that can't be deleted, a tested restore and a one-page list of who to call.

12 to 21 ticked: You've got a decent foundation. Now focus on practice, written instructions and your communication plan.

22 to 28 ticked: You're in good shape. Keep practicing and keep your plan fresh.

Want a hand building or testing your plan?

Mother Technologies helps businesses across Aberdeen, Edinburgh, Glasgow and the rest of Scotland build disaster recovery plans that are realistic, tested and the right size. Get in touch for a friendly, no-obligation chat at www.moherithech.co.uk