

Small business IT | Medium | 1 min read

Disaster recovery on one page

A **disaster recovery plan** says what you will do if IT stops working: fire, flood, theft, ransomware or a failed system. It does not need to be long. One clear page is far better than none.

What to put on the page

1. Contacts

- Who makes decisions, and their phone numbers.
- Your IT provider, broadband provider, bank, insurer and software suppliers.
- Keep a printed copy, since you may not be able to reach files on screen.

2. Your critical systems

List the three to five things you must get back first, such as email, accounts software, customer records, phones and the website. Give each an **order** and a rough time you could manage without it.

3. Where the backups are

- What is backed up, how often, and where.
- Who can restore it, and where the passwords and recovery keys are kept safely.

4. Where you will work

- Can people work from home, a laptop, or a temporary space?
- Do you have a spare laptop, and a way to take payments?

5. How you will tell people

- Staff, customers and suppliers: who tells them and how.
- A prepared message helps.

First steps in an emergency

1. Make sure people are safe.
2. Stop the problem spreading by disconnecting affected devices.
3. Call the right contact from the page.
4. Write down what happens and when.

Keep it alive

- Review the page twice a year.
- **Test restoring** a backup.
- Update it when staff or systems change.

When to get more help

Ask for help if you do not know how long a restore would take, if your backups have never been tested, if you depend on one person who knows everything, or if you want to practise a drill.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.