



BITWISE-IT BUSINESS TOOLKIT

Disaster Recovery Planner

Print it, fill it in, keep a copy somewhere else

Bitwise-IT Limited

Wickford, Essex · 01268 218301
info@bitwise-it.co.uk · bitwise-it.co.uk

How to use this planner

This is meant to be printed and filled in by hand. A recovery plan that exists only on the computer is not much use on the day the computer is the problem.

You do not need a forty-page document. You need one or two sheets that answer four questions: what matters most, how long you can manage without it, where the copies are, and who to ring. An hour spent here is worth more than any amount of good intentions.

When it is filled in, print two copies. Keep one at the office and one somewhere else entirely — at home, or with your accountant. Review it once a year, and whenever something significant changes.

1. What the business cannot run without

List your most critical systems and data in order. For each, note how long you could realistically cope without it before the business is in genuine trouble, and how much recent work you could afford to lose.

System or data	Time we could cope	Work we could lose	Where it lives

WHY THOSE TWO COLUMNS MATTER

They are the two numbers every recovery decision hangs on. "We could manage two days without email but only two hours of lost invoicing work" tells you immediately where to spend money and where not to. Most businesses have never articulated it, and end up protecting everything equally — which usually means protecting nothing well.

2. Where the copies are

What is backed up	Where the copy is	How often	Who checks it

If any row has a blank in the last column, that is not a backup — it is an assumption.

3. Who to call

Fill this in now, while everything is calm. On the day, nobody can remember anything and half of it is stored in the system that is down.

Who	Name	Number
IT support		
Internet provider (with account number)		
Phone provider		
Insurer (and policy number)		
Bank (fraud line)		
Accountant		
Landlord or building		
Key supplier		
Key client to notify		
Report Fraud (live cyber attack, 24/7)	Action Fraud	0300 123 2040
ICO (personal data breach, 72 hours)	ico.org.uk	0303 123 1113

4. Who does what

Role on the day	Who	Backup person
Decides what happens (the person in charge)		
Talks to IT support and suppliers		
Tells staff what is going on		
Tells clients what is going on		
Keeps the written record of events		
Handles insurance and any reporting		

How we will reach each other if email and phones are down

A group chat on personal phones is unglamorous and works. Agree it in advance, and make sure everyone is in it.

5. Work through the scenarios

Take each in turn and write down what you would actually do. Vague answers here are the point of the exercise — they show you exactly where the plan does not yet exist.

The office is inaccessible — fire, flood, or no power

A key computer or server has failed

Ransomware, or a serious security incident

Someone deleted something important, and nobody noticed for a week

A key person is unavailable for a month

A critical supplier or cloud service is down for two days

6. The first hour, whatever has happened

1. **Make sure everyone is safe.** Nothing on this page matters more than that.
2. **Work out what is actually affected** — and, just as importantly, what is not.
3. **Stop it spreading.** For anything security-related, disconnect from the network but leave machines powered on.
4. **Call IT support.** Early. Before trying anything clever.
5. **Tell your team** what is happening and what you want them to do, or not do.
6. **Start writing things down.** Times, actions, decisions, who was told what.
7. **Notify your insurer** if there is any chance of a claim — most policies require it promptly.
3. **Consider your reporting duties.** Personal data involved may mean the ICO within 72 hours.
9. **Tell clients before they find out another way.** Handled well, this costs far less trust than silence.

7. Keeping the plan alive

- ☐ Printed copies exist in two different places
- ☐ Everyone named in it knows they are named in it
- ☐ A restore has been tested since the plan was written
- ☐ It has been reviewed within the last twelve months
- ☐ It was updated when people, systems or suppliers last changed

Plan written: _____

Last reviewed: _____

Next review due: _____

THE BAR IS LOWER THAN YOU THINK

Businesses that come through these events well are almost never the ones with the most sophisticated plan. They are the ones who had a tested backup, knew who to call, and had agreed in advance who makes the decisions. Two sides of paper, filled in honestly, puts you ahead of most.

Want help filling this in?

We do this with clients as a matter of course — working out what actually matters, what the realistic recovery times are, and whether the current arrangements would stand up on the day. It usually takes an hour or two and it is the sort of thing that quietly repays itself many times over.

01268 218301 · info@bitwise-it.co.uk · bitwise-it.co.uk