Business continuity plan

A template to adapt for your business

Woodruff Training • woodrufftraining.com

Business name	Plan owner	Date and version

This is the plan for carrying on when something stops us working: a fire, a flood, a week without the internet, a ransomware attack, or the one person who knows how the invoicing works being in hospital. It is written to be picked up and used by whoever is available, not only by the person who wrote it. Fill in the blanks while nothing is wrong, because that is the only time anybody has the patience to do it.

1. What this plan is for

- It sets out how we keep the important parts of the business going during a disruption, and how we get back to normal afterwards.
- It covers everything we do, from every place we work, unless we have written an exception below.
- It sits alongside our insurance and our fire and health and safety arrangements. It does not replace any of them.
- It is deliberately short. A plan nobody has read is worth nothing at eight in the morning with the shutters down.

Anything this plan does not cover, and where that is dealt with instead

2. Who owns it, and who can put it into action

- One named person owns this plan and keeps it up to date. A second person can act in their absence, and knows they can.
- Either of them can decide the plan is in force. Nobody has to wait for permission from anyone else, and nobody is criticised afterwards for calling it too early.
- Say clearly when the plan is in force, and say clearly when normal working has resumed. People need to hear both.

Plan owner, deputy, and how to reach both of them out of hours

3. The first hour

In order. Do not move down the list until the one above is done.

- Check that everybody is safe and accounted for. Nothing on this page matters more than that.
- Call the emergency services if there is any risk to people or to the building.
- Get word to the plan owner or the deputy, by whatever means still works.
- Write down what has happened and the time. Keep writing as things develop. Memory becomes unreliable quickly, and insurers ask.
- Tell staff something, even if it is only that they should stay at home and we will ring by nine.
- If money may be moving, ring the bank before anything else.

For a suspected cyber incident specifically, there is a separate one-page card covering what to do and what not to do in the first hour, including why disconnecting is right and switching off is not.

4. What we cannot afford to lose

Not everything we do: the handful of things that start hurting within days. For each one, be honest about how long we could really cope without it before we lose customers, break a contract, or fail to pay somebody.

What we must keep doing	Who looks after it	How long we could cope	What it needs to work

The last column is the one people skip and then regret. It means the specifics: which system, which supplier, which spreadsheet, which member of staff, which key.

5. What could stop us

The causes are usually unexciting. Work through the list and write down what we already do about each, which is often more than we think.

What could stop us	Likely?	What we already do about it	What else we could do

Prompts: losing staff, losing access to the premises, losing computers or data, losing power, internet or phones, losing a key supplier, and being unable to travel. There are four honest answers to any of these: reduce it, insure or contract it away, stop doing the risky thing, or accept it. Accepting a risk is a perfectly good answer as long as somebody has actually decided it rather than never having looked.

6. Losing what we depend on

Two lines each. Where do people go, who arranges it, and how long does it take?

If we lose the premises, for a day or for a month

If we lose a key person, or several people at once

If we lose our computers, our systems or our data

If we lose power, internet or the phone line

If we lose a supplier or a customer we depend on

On the data line, write down where the backup actually is, who has ever restored from it, and how long that took. A backup nobody has tested is a hope, not a plan.

7. Who we need to ring

Fill this in now and print it. A contact list that only exists on a phone in a locked building is not a contact list.

Who	Name	Phone	Alternative

Include at least: every member of staff and a next of kin, IT support, the insurer and the policy number, the bank, the landlord, the utilities, the main suppliers, the biggest customers, the accountant and the local council.

8. The emergency pack

One box or folder, kept somewhere other than the office, containing the things that are useless if they are locked inside the problem.

- [ ] A printed copy of this plan, contact list included
- [ ] Insurance details and the claims number
- [ ] Staff contacts, including next of kin
- [ ] Customer and supplier contacts
- [ ] Bank and finance details
- [ ] Where the backups are, and how to get at them
- [ ] Spare keys and alarm codes
- [ ] A site plan showing the gas, electricity and water shut-offs
- [ ] Charged power bank, torch, pens and paper

> Check it twice a year. Contact lists go stale faster than anything else in this document.

The pack is kept here, and this person checks it

9. Telling people

- Staff first, and more often than feels necessary. Silence gets filled with something worse than the truth.
- Then any customer whose work is affected, before they notice and ring us.
- One person speaks for the business. Agree who now, so that nobody improvises to a journalist or on social media.
- If personal data may have been lost or exposed, check the reporting duties early. The deadline for notifying the Information Commissioner about a reportable personal data breach is 72 hours from becoming aware of it, which goes quickly while you are still working out what happened.

Who speaks for us, and who briefs staff

10. Keeping this worth having

- Review it once a year, and again after anything that actually happens.
- Talk it through with the team for half an hour a year. Reading a plan is not the same as having used one, and the gaps only show up when somebody asks who has the key.
- Update it whenever somebody leaves, a supplier changes, or we move.
- Keep one copy printed and one somewhere other than the office.

Reviewed on / by whom / next review due

11. Log of decisions and costs

Start this the moment the plan is in force. Nobody successfully reconstructs it afterwards, and the insurer will ask.

Date and time	What we decided or did	Who	Cost

Where this comes from. The structure follows the Cabinet Office Business Continuity Management Toolkit, which sets out what a continuity plan should contain but includes no template of its own, on the grounds that no single plan suits every organisation. The wording here is ours, and it has been cut down to what a small business will realistically fill in. The toolkit itself is free and worth reading if you want the fuller version. gov.uk: resilience in society, infrastructure, communities and businesses

Before you adopt this. This is a template to adapt, not legal, insurance or health and safety advice. Work through it with the people who would actually be holding it, change anything that does not match how you really operate, and delete what does not apply. Check the parts that touch your insurance against your own policy, because cover and notification requirements differ.