

Business Continuity Plan

Policy · UK · Updated 2026-07-11 · Square brackets are placeholders to replace with your own details.

A business continuity plan is the written playbook for keeping your business running — or getting it back running — when something serious goes wrong: the premises are unusable, the IT is down, a key supplier fails, or half the team is off at once. It answers, in advance, the questions that are hardest to answer mid-crisis.

Small businesses rarely fail because of the incident itself; they fail in the weeks after, when trading stops and nobody knows who decides what. A plan that fits on a few pages, with named people and current phone numbers, outperforms a binder nobody has opened.

This template covers the scenarios worth planning for, who takes charge, how you communicate, what gets recovered first, and how the plan is tested.

Purpose and scope

This plan sets out how [Your company] responds to serious disruption to normal operations at [site(s)]. It covers incidents that stop or significantly reduce our ability to trade, serve customers, or pay staff — not routine operational problems.

It applies to all staff. The current version is held at [location] and a copy is accessible off site at [location/system], because the plan is useless if it is locked inside the incident.

Policy statement

[Your company] is committed to protecting the safety of its people first, then its ability to serve customers and meet its obligations to staff, suppliers, and regulators. We will plan for disruption honestly, keep the plan current, and test it rather than assume it works.

Roles and responsibilities

- Continuity lead ([name/role]): invokes this plan, leads the response, and is the single decision-maker during an incident. Deputy: [name/role].
- Communications owner ([name/role]): handles messages to staff, customers, and suppliers using the arrangements in this plan.
- [Name/role]: owns IT and data recovery, including backups and data breach assessment.
- All staff: know where the plan is kept, follow the communications channel below, and do not speak to press or post about incidents on social media.

Scenarios we plan for

- Premises unusable (fire, flood, damage, denial of access): fallback is [alternative site / remote working / mobile arrangement].
-

IT failure or cyber attack: fallback is [backup and restore arrangement, manual workaround — e.g. paper order pads, backup card terminal].

- Loss of utilities (power, water, gas): fallback is [arrangement, e.g. safe shutdown steps and temporary closure criteria].
- Key people unavailable (illness, resignation, emergency): critical tasks and deputies are listed under recovery priorities.
- Key supplier failure: alternative suppliers for [critical items] are listed in the contacts annex.

Invoking the plan

1. Make people safe first: follow the emergency procedures for the incident (evacuation, first aid, 999) before anything in this plan.
2. The continuity lead (or deputy) decides whether to invoke the plan and records the decision and time.
3. Assemble the response team — in person or on [channel] — and assess what is affected, for how long, and what can still run.
4. If personal data may be involved, start the data breach response procedure immediately — the 72-hour ICO clock runs from awareness.
5. Notify the insurer ([name/policy number]) and landlord [if applicable] before authorising clean-up or repairs beyond making things safe.
6. Work through the recovery priorities below, log every decision and expense, and reassess at least daily.

Communications during disruption

Staff are contacted through [channel — e.g. WhatsApp group or phone cascade] by the communications owner; the staff contact list is kept current at [location]. Tell staff what happened, whether to come in, and when the next update will come — silence fills itself with rumour.

Customers are told the practical truth — what is closed or delayed and when to expect an update — through [website, social channels, signage, direct contact for bookings]. Only the communications owner or continuity lead speaks for the business.

Recovery priorities

- Within [number] hours: [e.g. make the premises safe, secure stock and cash, contact all staff, redirect deliveries].
- Within [number] days: [e.g. restore payment and till capability, resume core service even if reduced, contact key customers and suppliers].
- Within [number] weeks: [e.g. return to full trading, replace equipment, progress the insurance claim, review what happened].
- Critical dependencies and deputies: [task — payroll, ordering, banking — with who does it normally and who can cover].

Testing, records and review

The plan is tested at least [frequency, e.g. annually] with a walkthrough of one scenario, and contact lists are verified [frequency, e.g. quarterly]. Test findings, incident logs, and decision records are kept at [system/location].

The plan is reviewed [frequency], after every invocation or near-miss, and when premises, systems, key staff, or suppliers change. Owner: [name/role]. Next review due: [date].

How to use this template

1. Start with the shortest useful version: one page per scenario with names, numbers, and first actions — expand only where a real gap appears.
2. Fill in the contacts annex first (insurer, landlord, IT, bank, key suppliers, staff) and store a copy somewhere the incident cannot reach.
3. Set recovery time targets by asking how long you can stop trading before the damage is permanent — then build the priorities backwards from that.
4. Walk through one scenario with your response team before publishing; the walkthrough will surface the assumptions that are wrong.
5. Diary the contact-list check and the annual test now — an untested plan with stale numbers is a false sense of security.

Official guidance

- › [ICO — Report a breach](#)

This template is provided in good faith and for general information — it is not legal advice. Adapt it to your organisation and, where your sector carries specific legal requirements, have the finished document reviewed by a qualified adviser. The live version at <https://trainedteam.com/templates/business-continuity-plan> is kept current; this file is a snapshot.