AIS TECHNOLOGY

# Business Continuity Plan Template

For UK small and medium sized businesses

This template gives you a working business continuity plan without starting from a blank page. Every field can be typed into and saved in any PDF reader, or printed and completed by hand. Work through it in order: the later sections depend on decisions you make in the first two.

A plan nobody has tested is a document, not a capability. Once you have filled this in, book the first test in section 7 before you file it anywhere.

## 00 Plan details and version log

Keep this at the front so it is always clear when the plan was last reviewed and by whom.

**ORGANISATION**

**PLAN OWNER**

**DATE COMPLETED**

**NEXT REVIEW DUE**

| VERSION | DATE | REVIEWED BY | WHAT CHANGED |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Section 1: Critical functions register

List what your business actually does day to day, then be honest about how long each thing could stop before it causes real damage. Most businesses find they have three or four genuinely critical functions and a longer list of things that merely feel urgent.

> Rank by consequence, not by how loudly someone would complain. If payroll runs monthly, losing it for a day in the third week costs nothing and losing it on run day costs a lot.

| BUSINESS FUNCTION | OWNER | DEPENDS ON (SYSTEMS, PEOPLE, SUPPLIERS) | PRIORITY |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Section 2: Business impact analysis

For each critical function, set a recovery time objective and a recovery point objective. The RTO is how long it can be offline before the impact is unacceptable. The RPO is how much recent data you could afford to lose and recreate.

> These two numbers drive everything you spend. An RPO of one hour means backups every hour; an RPO of 24 hours means nightly is fine. Set them from the cost of the outage, then check your current setup can actually meet them. If it cannot, that gap is your action list.

| FUNCTION | IMPACT OF LOSING IT | RTO | RPO | CAN WE MEET IT TODAY? |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Section 3: IT systems and recovery procedures

One row per system that matters: email, file storage, accounting, your line of business application, phones, the website. Record where the backup lives and who is able to restore it. Build the procedure around remote access as the default, because the office may be the thing that is unavailable.

| SYSTEM | PROVIDER / LOCATION | BACKUP LOCATION | WHO CAN RESTORE IT | LAST TESTED |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 3.1 Backup checks

The 3-2-1 rule is the industry standard and the single most effective safeguard you can put in place: three copies of your data, on two types of media, with one copy offsite or in the cloud. Tick these off honestly.

- [ ] We hold at least three copies of business critical data.
- [ ] Copies exist on at least two different types of media or platform.
- [ ] At least one copy is offsite or in a separate cloud tenancy.
- [ ] We have restored from backup successfully in the last three months.
- [ ] Backup failures raise an alert that a named person acts on.
- [ ] Backups are protected from ransomware, for example immutable or air gapped.

# Section 4: Emergency contacts

Include mobile numbers and at least one contact method that does not depend on your own email or phone system, because those may be exactly what is down. Print a copy and keep it somewhere that does not require a working network to reach.

| NAME | ROLE IN AN INCIDENT | MOBILE | ALTERNATIVE CONTACT |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 4.1 External contacts

IT support provider, internet provider, insurers, bank, landlord, key suppliers, and your data protection contact for reportable breaches.

| ORGANISATION | WHAT THEY COVER | ACCOUNT OR POLICY NUMBER | CONTACT |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

> Under UK GDPR a personal data breach that risks people's rights must be reported to the ICO within 72 hours of you becoming aware of it. Decide now who makes that call, and write their name in the table above.

# Section 5: What we do in the first hour

The point of a plan is that nobody has to invent a response while under pressure. Keep these steps short enough that a stressed person can follow them.

| STEP | ACTION | WHO DOES IT | DONE |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 5.1 Declaring an incident

Write down who has the authority to declare an incident and start this plan, and who deputises when that person is unavailable.

**WHO CAN DECLARE AN INCIDENT**

**DEPUTY**

**WHERE THE TEAM GATHERS, PHYSICALLY OR ONLINE**

# Section 6: Communication

Decide in advance what you will tell staff, clients and suppliers, and who says it. Silence during an outage does more reputational damage than the outage itself.

| AUDIENCE | WHO TELLS THEM | HOW (CHANNEL THAT WILL STILL WORK) | WITHIN |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 6.1 Holding statement

Draft it now, while nothing is on fire. Keep it factual and avoid speculating about cause.

# Section 7: Testing schedule and log

Review the plan at least annually, and whenever something significant changes: a new office, a cloud migration, a change of IT provider, a new system, or new people in key roles. A tabletop walkthrough with the team counts as a test and takes an hour.

| DATE | TYPE OF TEST | SCENARIO | WHAT FAILED OR SURPRISED US | ACTION TAKEN |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 7.1 After each test

- [ ] Contact details in section 4 are still correct.
- [ ] RTOs and RPOs still match what the business needs.
- [ ] Recovery procedures still match the systems we actually run.
- [ ] Lessons from the test have been written back into this plan.
- [ ] The version log on page 1 has been updated.

### Not sure your plan would survive a real incident?

We regularly find businesses with backups that have never been tested, admin passwords nobody can locate, and recovery procedures that assume the office is still standing. A short conversation will tell you which of those applies to you.

**aistech.co.uk/contact | +44 204 591 6648 | info@ais.london**