

Disaster recovery and business continuity plan

[Organisation name]

Plan owner	Version	Approved by	Date approved	Next review

How to use this template: replace everything in [square brackets], fill the tables, and delete the guidance notes in italics. Keep a copy of the finished plan somewhere you can reach when your systems are down, such as a printed copy and a copy on a phone that is not joined to your network. The structure follows UK guidance: the NCSC says an incident response plan should sit alongside inter-linked business continuity, disaster recovery and communications plans, and AWS advises that the disaster recovery plan should be a subset of the business continuity plan rather than a standalone document. This template puts both in one place.

1. Purpose and scope

This plan sets out how [organisation] keeps its critical business processes running during a serious disruption (business continuity) and how it recovers its IT systems and data afterwards (disaster recovery).

It applies to: [sites, teams, systems and suppliers in scope].

It is invoked when: [the events that trigger it, for example loss of a site, loss of the network or a core system for longer than X hours, a ransomware or other cyber attack, or the failure of a critical supplier].

A backup is a copy of your data. Disaster recovery is the plan for getting systems running again after a major failure. Business continuity is the wider plan for keeping the business going, including people, premises and manual processes. Write the plan so that it still works if the people who wrote it are away.

2. Roles and contacts

The NCSC says to consider the risk of people being unavailable, and ideally include at least two contact methods and two or more people for each contact. Use numbers that work out of hours. Record one conference call number or alternative channel that stays available when email and phones are down.

Role	Name	Deputy	Phone	Second contact method
Plan owner and incident lead				
Deputy incident lead				
Senior decision maker (can declare a disaster, take systems offline, approve spend)				
IT lead				
Backup and restore lead				
Communications (staff, customers, suppliers, press)				
Legal and data protection (DPO)				
HR				
Finance and insurance claims				

Role	Name	Deputy	Phone	Second contact method
IT provider or MSP				
Backup vendor support (contract or licence number)				
Cyber insurer or broker (policy number)				
Incident response provider (NCSC assured scheme, if retained)				
Landlord, utilities, building security				
Key suppliers				
Key customers or regulators to inform				

Always-available conference line or alternative channel: [number or service, and who can start it]

Reporting contacts (UK)

Who	When	How
ICO (Information Commissioner's Office)	If personal data is affected and the breach is likely to pose a risk to people: as soon as possible and where feasible within 72 hours. If the risk to people is high, tell those people without undue delay.	ico.org.uk, online breach report form (about 30 minutes, cannot be saved part-way)
NCSC	Any cyber incident affecting a UK organisation	gov.uk/report-cyber, which routes you to the right reporting service
Report Fraud (formerly Action Fraud)	Cyber crime and fraud in England, Wales and Northern Ireland. A business, charity or organisation under a cyber attack: call immediately.	actionfraud.police.uk, 0300 123 2040. In Scotland report to Police Scotland on 101.
Cyber insurer or broker	As soon as an incident is suspected; the policy may require it before you spend money on response	[policy number and claims line]
Other regulators and contracts	[FCA, Ofcom, NHS, sector regulators, customer contracts with notification clauses]	[details]

3. Business impact analysis

List each business process, who owns it, how critical it is, and how long the business can be without it (the maximum tolerable downtime, MTD). Microsoft recommends classifying workloads into tiers by their importance to the business, and AWS recommends a business impact analysis that quantifies the impact of a disruption and shows how quickly a workload must be available and how much data loss can be tolerated. Impact depends on timing: a payroll outage matters far more just before payday.

Business process	Owner	Tier (1 = most critical)	MTD	Systems and suppliers it depends on	Manual workaround while it is down
[e.g. taking and fulfilling orders]		1	[e.g. 8 hours]	[e.g. ERP, email, payment provider]	[e.g. paper order forms, phone orders]
[e.g. paying staff]		2	[e.g. 3 days, 1 day in payroll week]		

Business process	Owner	Tier (1 = most critical)	MTD	Systems and suppliers it depends on	Manual workaround while it is down

4. Risks and how they are treated

Microsoft suggests treating common risks (a failed disk, a single server) with high availability and uncommon risks (loss of a site, a region outage, ransomware) with disaster recovery. Add the risks that apply to you and delete the rest.

Risk	Likelihood (L/M/H)	Impact (L/M/H)	How it is treated (prevention, high availability, this plan)	Owner
Ransomware or other destructive cyber attack			[offline or immutable backups, MFA, patching, Cyber Essentials; sections 6 and 7]	
Loss of a site (fire, flood, access denied)			[remote working, alternative premises; section 7]	
Power, internet or network outage				
Cloud or SaaS provider outage (Microsoft 365, Google Workspace, hosting)				
Critical supplier failure				
Hardware failure or data corruption				
Human error (deleted data, bad change)				
Loss of key people				

5. Systems, recovery targets and backups

RPO is the most data you can afford to lose, measured in time. RTO is how long the system can take to come back. Both come from the business impact analysis, not from what the backup software happens to do. Check them with the free RPO and RTO calculator at futuretechnologyhq.com/tools/rpo-rto-calculator/. The NCSC says to always have a recent offline backup of your most important files and data, and that MFA for backups should not be on the same device used to administer them.

System or data set	Tier	RPO	RTO	Backup method and frequency	Where the copies are (include the offline or immutable copy)	Restore order
[e.g. file server]	1	[24 h]	[8 h]	[nightly image, hourly file sync]	[local NAS; immutable cloud bucket; monthly offline disk]	2
[e.g. Microsoft 365 mail and SharePoint]	1			[third-party backup, 3 times a day]		1

Where the credentials, encryption keys and licence details needed for a restore are kept, offline and reachable without the network: [location and who holds it]

6. Disaster recovery procedures

6.1 Declaring a disaster

Who can declare a disaster and invoke this plan: [named roles, with deputies]. How they are reached out of hours: [details]. What they tell the team first: what has happened, which processes are affected, which part of this plan is active, and when the next update is.

6.2 First actions

- ☐ Make sure people are safe. If there is a physical emergency, call 999 first.
- ☐ Start the incident log (appendix A). Record decisions, actions and times offline, on a system the incident cannot reach.
- ☐ Assess what is affected: which processes, systems, sites and data, and whether personal data may be involved.
- ☐ Contain the damage: isolate affected systems, stop replication or sync jobs that could spread the problem to good copies, and protect the backups.
- ☐ Switch to the manual workarounds in section 3 for the processes that cannot wait.
- ☐ Tell the people in section 2 who need to know, in the order the senior decision maker sets.
- ☐ Make the reports in section 2 within their deadlines, starting with the insurer and, where personal data is involved, the ICO assessment.
- ☐ Decide the recovery order from section 5 and assign each restore to a named person.

6.3 Recovery runbook

Copy this table once per system, in restore order. Write it so that someone who did not build the system could follow it. Restoring data is not enough: you also need somewhere to restore to, so record how the infrastructure, configuration and application code are rebuilt (AWS's point about backup-and-restore recovery).

Step	Action	Who	Done (time)
1	Confirm the restore target is clean and ready (hardware, VM, cloud account, network)		
2	Get the credentials and keys from the offline store		
3	Choose the restore point (check it predates the problem and that the copy is intact)		
4	Rebuild the platform: [OS, configuration, application code, licences]		
5	Restore the data from [which copy]		
6	Check the data: [sample records, latest transactions, file counts, application starts]		
7	Reconnect users and dependent systems		
8	Tell the process owner the system is back and record the time		

6.4 If the cause is ransomware or another attack

- ☐ Do not restore until you are confident the attacker has been removed. The NCSC says to confirm that remediation has been successful before moving to recovery, which may involve monitoring for a period.

- ☐ Restore from the offline or immutable copy, and check it is free of the attacker's tools before reconnecting it.
- ☐ Reset credentials, especially administrator and service accounts, before systems go back online.
- ☐ Do not pay a ransom without objective expert advice. The NCSC and UK law enforcement do not encourage, endorse or condone paying ransom demands.
- ☐ Use the separate ransomware response checklist (futuretechnologyhq.com/article/ransomware-recovery-incident-response-plan/) for the hour-by-hour steps and the UK reporting routes.

7. Business continuity arrangements

7.1 Premises and people

If the main site is unavailable: [alternative premises, home working, which teams go where, how equipment is issued].

Staff welfare and working hours during the incident: [who checks on people, cover for long shifts, what staff are told to do if they cannot work].

7.2 Communications plan

The NCSC says to consider secure or alternative communications for when normal channels are unavailable because of a network, email or phone outage. Decide in advance who speaks for the organisation; one voice for customers and the press.

Audience	What they need to know	Who tells them	Channel (and the backup channel)	How often
Staff			[e.g. SMS group, personal email list, phone tree]	
Customers				
Suppliers and partners				
Insurer, regulators, police				
Press and public				

7.3 Manual processes

For each tier 1 process in section 3, the manual workaround in detail: where the forms are, who is trained, how the records are kept so they can be entered into the systems afterwards. [Attach or list]

7.4 Money

How urgent payments are made if finance systems are down, who can authorise emergency spend, and what the cyber insurance policy covers and requires: [details].

8. Return to normal

- ☐ The criteria for standing the plan down: [which systems and processes are back, and who confirms it].
- ☐ Manual records made during the disruption are entered into the systems and reconciled.
- ☐ Temporary access, accounts and workarounds are removed.

- ☐ A post-incident review is held. The NCSC says it should cover lessons from the incident itself and lessons from the response, across people, process and technical capabilities.
- ☐ This plan, the contact list and the runbooks are updated with what was learned, and the changes are tested.

9. Testing and maintenance

AWS says it is critical to regularly assess and test your disaster recovery strategy so that you have confidence in invoking it. Microsoft says business continuity planning is a process, not a one-time event. Review this plan at least once a year and after any major change to systems, suppliers or people. The NCSC's free Exercise in a Box has ready-made ransomware and other exercises. How often to test, and which kind of test to run, is covered at futuretechnologyhq.com/article/how-often-test-disaster-recovery-plan/.

Test	Frequency	Last run	Result	Actions and owner
Contact list check (every number answered)	[quarterly]			
Restore test of a tier 1 system from the offline or immutable copy	[quarterly]			
Table-top walkthrough of a scenario with the incident team	[twice a year]			
Full recovery or failover exercise	[yearly]			
Plan review and re-approval	[yearly and after major change]			

10. Document control

Version	Date	Author	Change	Approved by
1.0			First issue	

Copies of this plan are held: [printed copy at ..., offline copy with ..., copy with the IT provider]. Anyone holding a copy gets each new version.

Appendix A. Incident log

The NCSC says a careful record of decisions, actions and data captured is useful for post-incident reviews, especially if you need to show your response to a regulator. Keep it offline during a cyber incident.

Date and time	Event, decision or action	Who	Notes and evidence

Date and time	Event, decision or action	Who	Notes and evidence

Version 1.0, 27 October 2026. Free template from Future Technology, futuretechnologyhq.com. Use and adapt it freely; it is general guidance, not legal advice.