IT disaster recovery plan template

For UK organisations on Microsoft 365, Azure and on-premises servers

Template version 1.0, 16 November 2026

> **How to use this template:** Replace the grey examples with your own details, and delete any rows or scenarios that don't apply. Keep at least one copy outside Microsoft 365, printed or on a device that doesn't depend on it, so you can still open the plan when Microsoft 365 or your network is down. Review the plan by the date in Plan details, and after every test and every incident.

Text in grey is an example: write your own beside it, or in the blank rows.

Latest version: computecloud.co.uk/tools/it-disaster-recovery-plan-template/

Licence: IT disaster recovery plan template by ComputeCloud (computecloud.co.uk), CC BY 4.0 (licence terms). You may adapt it for your own organisation.

In this plan

1. Plan details 2
2. Roles and contacts 2
3. Systems and priorities 4
4. Backups 5
5. Scenarios 6
6. Testing log 11
7. After an incident 11
Appendix A. Microsoft's SLA 12
Appendix B. Example: scenario a filled in for the 12 November 2026 Microsoft 365 outage 14

1. Plan details

How to fill it in: Say who owns the plan, which version this is and when it will next be reviewed. Keep at least one copy where you can reach it without Microsoft 365: the NCSC advises keeping plans, checklists and contact details available for when you can't get into your computer systems.

What to record	Example	Yours
Organisation	[Organisation name]	
What this plan covers	[Offices, teams and systems covered, for example our office in [town], Microsoft 365, one server in Azure]	
Plan owner	[Name], [job title]	
Deputy owner	[Name], [job title]	
Approved by	[Name], Managing director	
Version	[1.0]	
Date of this version	[Date]	
Next review date	[Date]	
Who holds a copy	[Plan owner, deputy owner, IT support provider]	
Master copy kept in	[SharePoint site or folder]	
Copy kept outside Microsoft 365	[Printed copy with the plan owner, and a PDF on a phone or a USB stick kept off the network]	

Keep a printed copy. If Microsoft 365 is down or your network has been attacked, the copy in SharePoint or OneDrive may be the one you can't open.

2. Roles and contacts

How to fill it in: Name who declares a disaster and who does each job, with a deputy for each. Write down how you'll reach people if email and Teams are down: the NCSC suggests alternative channels such as phone lines or messaging apps, and an offline copy of contact lists for key staff, suppliers and partners.

Roles

Role	Name and deputy	What they do	How to reach them without email or Teams
Declares a disaster and leads the response	[Name], Managing director. Deputy: [Name]	Decides when to invoke the plan, approves spending, signs off messages to customers	[Mobile number]
Technical lead	[Name], IT lead, or [IT support provider]	Checks Service health, contains the problem, restores systems and data	[Mobile number]

Role	Name and deputy	What they do	How to reach them without email or Teams
Communications	[Name], Office manager. Deputy: [Name]	Tells staff, customers and suppliers what's happening and when the next update is due	[Mobile number]
Recorder	[Name]	Keeps the incident log: what was found and when, decisions taken, by whom and why	[Mobile number]
Data protection lead	[Name]	Decides whether a personal data breach must be reported to the ICO	[Mobile number]

What to record	Example	Yours
We invoke this plan when	[For example: a system in priority tier 1 is down for longer than its RTO, any sign of ransomware, or the office can't be used]	
Who can invoke it	[Managing director, or the deputy if they can't be reached]	

Reaching staff when email and Teams are down

What to record	Example	Yours
Main channel	[For example: a group text message, or a messaging app group on work phones]	
Backup channel	[For example: a phone tree, where each manager calls their own team]	
Who sends the messages	[Name], Office manager	
Where the staff contact list is kept	[Printed with the plan; exported from the HR system on [date]]	
First message to staff	[We have a problem with [system]. [What still works]. Next update by [time] on [channel].]	

Supplier contacts

Supplier	What they provide	Account or contract number	Phone	Notes
[Internet provider]	Office internet connection	[Account number]	[Fault line]	[Fault reporting hours]
[IT support provider]	Support for laptops, Microsoft 365 and servers	[Contract number]	[Phone]	[Support hours and out-of-hours number]
[Microsoft licensing partner]	Microsoft 365 and Azure subscriptions	[Tenant name]	[Phone]	[Who raises an SLA claim]

Supplier	What they provide	Account or contract number	Phone	Notes
[Insurer]	Cyber insurance	[Policy number]	[Incident line]	[What must be reported, and how soon]
[Software supplier]	[Accounts or line-of-business software]	[Account number]	[Phone]	[Where our data is held]

Where to report an incident (checked 16 November 2026; check these each time you review the plan):

- **A business under a cyber attack in England, Wales or Northern Ireland:** phone Report Fraud on 0300 123 2040 straight away, as it asks businesses under attack to do. Report Fraud is the new name for Action Fraud and is run by the City of London Police. Other cyber crime and fraud can be reported online at reportfraud.police.uk.
- **In Scotland:** Police Scotland isn't part of Report Fraud. Call 101, use its online form, or report in person.
- **The NCSC:** report a cyber incident at report.ncsc.gov.uk. The NCSC says this doesn't meet any legal or regulatory duty to report, and it won't pass information to regulators without your consent. GOV.UK's where to report a cyber incident service helps you work out who else to tell.
- **The ICO, for a personal data breach:** if a breach is likely to put people's rights and freedoms at risk, report it within 72 hours of becoming aware of it, where feasible, with whatever you know so far. The clock starts when you discover the breach, not when it happened. Report a breach to the ICO.
- **Your insurer:** as your policy requires. Note its deadline in the supplier table above.

3. Systems and priorities

> **How to fill it in:** List every system the business needs, starting with the ones it can't work without. **RTO** (recovery time objective) is how long a system can be down; **RPO** (recovery point objective) is how much data, measured in time, you can afford to lose. These are your business's choices, so agree them with the people who use each system: the NCSC says the needs of the business, not only IT, should decide what is restored first.

Systems and priorities

System and owner	Where it runs	What depends on it	RTO (how long it can be down)	RPO (how much data you can lose)	Priority tier
Sign-in and accounts (Microsoft Entra ID). Owner: [Name]	Microsoft 365	Everything that uses a Microsoft 365 sign-in	Example: 1 hour	Example: not applicable	1
Email and calendars (Exchange Online). Owner: [Name]	Microsoft 365	Quotes, customer contact, Teams calendar and scheduling	Example: 4 hours	Example: 1 hour	1
Files (SharePoint and OneDrive). Owner: [Name]	Microsoft 365	Every team's documents	Example: 1 day	Example: 1 day	1
[Accounts software]. Owner: [Name]	On-premises server	Invoicing and payroll	Example: 2 days	Example: 1 day	2

System and owner	Where it runs	What depends on it	RTO (how long it can be down)	RPO (how much data you can lose)	Priority tier
[Order system]. Owner: [Name]	Azure virtual machine	Orders and stock	Example: 8 hours	Example: 4 hours	1
[Phone system]. Owner: [Name]	Other cloud app	Customer calls	Example: 4 hours	Example: not applicable	1
Office internet connection. Owner: [Name]	Office	Every cloud service, when used from the office	Example: 4 hours	Example: not applicable	1

Priority tiers (change them to suit you): **1** restore first; **2** restore once tier 1 is back; **3** can wait until normal work has resumed.

> Write down what each system depends on, such as Microsoft 365 sign-in, the internet connection, a server or a supplier. The NCSC advises identifying which systems, and the systems they rely on, support your critical work and should be recovered first.

4. Backups

> **How to fill it in:** For each system, record what is backed up, where, how often and for how long, who can restore it and when you last tested a restore. The NCSC advises keeping backups separate from your network, in a different place or a cloud service designed for it, because ransomware targets backups, and checking that you know how to restore.

Backups

System	What's backed up	Where the backup is kept	How often	How long it's kept	Who can restore it	Last restore test
Microsoft 365	Mailboxes, OneDrive accounts and SharePoint sites	[Microsoft 365 Backup, or a third-party backup service]	[Daily]	[1 year]	[Name], IT lead	[Date]: restored [a deleted folder] in [time]
[Accounts software]	[Database and attachments]	[Azure Backup, plus a copy kept offline]	[Nightly]	[30 days]	[IT support provider]	[Date]
[Order system]	[The whole Azure virtual machine]	[Azure Backup]	[Daily]	[30 days]	[Name]	[Date]
Laptops	[Work files, kept in OneDrive]	[OneDrive]	[As files change]	[See Microsoft's windows below]	[Each user, or IT support]	[Date]

What Microsoft keeps if you have no backup. Microsoft 365 keeps deleted items for set periods so you

can undo mistakes. These are Microsoft's windows, not a backup.

What Microsoft keeps after something is deleted

What	Kept for
Deleted email, by default. An admin can raise it to 30.	14 days
Deleted files in the OneDrive and SharePoint recycle bin.	93 days
A deleted mailbox, before it is gone for good.	30 days
A leaver's OneDrive, by default (30 to 3,650).	30 days

From Microsoft's documentation, checked 31 October 2026. The sources are in our Microsoft 365 backup guide.

Microsoft says that for every type of cloud service you own your data and are responsible for protecting it. To go back further than these windows, or to recover from ransomware or a mass deletion, you need a backup: Microsoft 365 Backup, Microsoft's own pay-as-you-go add-on for Exchange, OneDrive and SharePoint, or a third-party tool. Our Microsoft 365 backup guide compares them.

For servers, Microsoft describes Azure Backup as a way to back up workloads in Azure and on-premises, and says it covers backup and restore, while Azure Site Recovery covers disaster recovery and failover. See Azure backup and disaster recovery.

> Don't leave backup drives connected to your network, and before you restore, connect backups only to devices you know are clean and scan them for malware. Both are NCSC advice for recovering from ransomware.

5. Scenarios

> **How to fill it in:** Each scenario has first steps, who acts and when to escalate. Change the steps to fit your systems, and delete any scenario that doesn't apply. Whatever happens, start the incident log straight away: the NCSC advises one record of what was found and when, which decisions were taken, by whom and why.

What to record	Example	Yours
Incident log kept in	[A notebook, or a document stored outside Microsoft 365]	

> Use UK time for every entry in the incident log, and note the time zone of anything you copy from a supplier.

a. Microsoft 365 outage

> **How to fill it in:** Use this when email, Teams or files stop working for several people at once. Check Microsoft first: Microsoft says to check Service health to see whether an issue is already known before you call support or spend time troubleshooting. Our guide to checking for a Microsoft 365 outage has the detail.

Before it happens

- Turn on Service health emails: in the Microsoft 365 admin centre, go to **Health** › **Service health** › **Customize** › **Email**. Each admin can add up to two addresses. Make one an address outside Microsoft 365, so a notice can still reach you if Exchange Online is down.

- Install the Microsoft 365 Admin app on admins' phones. Microsoft says it shows Service health, with push notifications.
- Check offline email is on. Classic Outlook uses Cached Exchange Mode by default, which keeps a copy of the mailbox on the computer; new Outlook for Windows has offline access, on by default (**Settings** › **General** › **Offline**). On Remote Desktop Services, Microsoft says new Exchange accounts use Online Mode by default, so those users have no offline copy.
- In OneDrive, mark the files people would need in an outage as **Always keep on this device**, so they open without a connection.

First steps

1. Check **Health** › **Service health** in the Microsoft 365 admin centre (admin.microsoft.com). If you can't sign in, check Microsoft's public status page, status.cloud.microsoft, or @MSFT365Status on X.
2. If an active issue matches what staff see, note its ID and select **Manage notifications for this issue** to get each update by email. If nothing matches, select **Report an issue**: the problem may be in your own setup or network.
3. Tell staff what's affected, what still works and when Microsoft's next update is due, using the channels in Roles and contacts if email or Teams is affected.
4. Keep working offline. Outlook can still show email it has already downloaded. Classic Outlook sends email written offline when it reconnects; new Outlook puts new messages in the Outbox. Files kept on the device still open.
5. Start a timeline for a possible SLA claim: when problems started and ended for you, how many users were affected and where, and the errors they saw. See the appendix on Microsoft's SLA.
6. When Microsoft says the service is restored, check that email is arriving and that queued messages have caught up. Save Microsoft's updates and its post-incident report: Service health keeps 30 days of history.

What to record	Example	Yours
Who acts	[Name], IT lead: Service health and Microsoft's updates. [Name], Office manager: messages to staff and customers.	
Escalate when	[Email is down for longer than its RTO, or Microsoft lists nothing and IT support can't find a local cause within an hour]	

b. Ransomware or malware

> **How to fill it in:** Use this if files are encrypted, a ransom demand appears, or devices behave strangely. The NCSC's guidance on recovering from a highly disruptive cyber attack covers the first hours in detail.

First steps

1. Decide quickly whether to disconnect affected devices from the network or shut them down. The NCSC says disconnecting can stop attackers sending further commands, limit the spread and preserve evidence, while shutting down can lose evidence. Take specialist advice if you can.
2. Call your IT support provider or a cyber incident response provider. The NCSC lists assured Cyber Incident Response providers.
3. Report it: in England, Wales or Northern Ireland, phone Report Fraud on 0300 123 2040 straight away; in Scotland, call Police Scotland on 101. Report it to the NCSC as well (see Roles and contacts).

4. If personal data may be affected, start the ICO clock: a reportable breach must be reported within 72 hours of becoming aware of it, where feasible.
5. Tell your insurer, as your policy requires.
6. Before you restore, check your backups: when were they last taken, are they still available and have they been compromised? Connect them only to devices you know are clean, and scan them for malware first.
7. Change passwords, starting with admin accounts, once your responder agrees it's safe. The ICO suggests changing passwords as one way to contain a cyber incident.

> The NCSC says paying a ransom doesn't guarantee you get your data back, and law enforcement doesn't encourage, endorse or condone paying. Practise this scenario with the NCSC's free ransomware tabletop exercise in Exercise in a Box.

What to record	Example	Yours
Who acts	[Name], Managing director: leads and decides. [IT support provider]: contains and restores. [Name]: reports to the ICO.	
Escalate when	[Immediately: treat any sign of ransomware as a disaster and invoke the plan]	

c. Loss of the office or server room

> **How to fill it in:** Use this if a fire, flood or power cut means people can't use the office, or the server room is damaged or without power.

First steps

1. Make sure everyone is safe and follow the building's emergency procedures before anything else.
2. Tell staff where to work, from home or [another site], using the channels in Roles and contacts.
3. Check what still works. Cloud services such as Microsoft 365 can usually be reached from home; systems on a server in the building can't.
4. Ask your IT support provider to restore on-premises systems from backup somewhere else, in the order in Systems and priorities.
5. Divert office phones, and update voicemail and the website if customers can't reach you.
6. Tell your insurer, and keep photos and a list of damaged equipment.

What to record	Example	Yours
Who acts	[Name], Office manager: staff and building. [IT support provider]: systems.	
Escalate when	[The office will be unusable for more than [1 day], or the server can't be restored within its RTO]	

d. Internet connection failure

> **How to fill it in:** Use this when the office loses its internet connection but Microsoft 365 itself is working. Microsoft's SLA doesn't cover a network failure at your site or between your site and Microsoft's data centre, so this one is yours to plan for.

First steps

1. Check whether it's just the office: can staff reach Microsoft 365 on a phone using mobile data?
2. Report the fault to your internet provider, and note the reference number and the estimated fix time.
3. Move people to a backup connection, such as [a 4G or 5G router or phone hotspots], or to working from home.
4. Staff can keep working from email Outlook has already downloaded and from files kept on their device.
5. If staff need a server in the office from elsewhere, use [our remote access method].

What to record	Example	Yours
Who acts	[Name], Office manager: reports the fault. [IT support provider]: backup connection.	
Escalate when	[The provider can't fix it within [4 hours], or the phones also depend on the connection]	

e. Compromised account or accidental deletion

> **How to fill it in:** Use this if an attacker is using someone's account, or email or files have been deleted, by mistake or on purpose. Microsoft's guide to responding to a compromised email account has the full steps for admins.

First steps: a compromised account

1. Disable the account while you investigate, and revoke its active sessions, as Microsoft advises.
2. Remove any sign-in (MFA) methods or devices you don't recognise, apps that shouldn't have access, and admin roles the account shouldn't have.
3. Remove any mail forwarding the attacker set up.
4. When the investigation is finished, reset the password and turn the account back on.
5. If personal data may have been exposed, decide whether to report it to the ICO (see Roles and contacts), and follow the NCSC's advice on hacked accounts.

First steps: deleted email or files

1. Email: the user can get deleted items back with **Recover Deleted Items** in Outlook or Outlook on the web, within the deleted item retention period (see Backups).
2. Files: restore them from the OneDrive or SharePoint recycle bin. To undo a lot of changes at once, Microsoft lets you restore a whole OneDrive, or a SharePoint document library, to any point in the last 30 days.
3. A deleted user: an admin can restore the user, and their mailbox, from **Deleted users** in the Microsoft 365 admin centre within 30 days.
4. Anything older than Microsoft's windows: restore from your backup.

What to record	Example	Yours
Who acts	[Name], IT lead, or [IT support provider]	
Escalate when	[An admin account is affected, the attacker sent email to customers, or data is beyond Microsoft's windows and has no backup]	

f. Azure virtual machine or region failure

> **How to fill it in:** Use this if a server you run in Azure stops working, or Microsoft reports a problem with an Azure region. Microsoft says that deploying to a region pair, such as UK South and UK West, doesn't by itself give you disaster recovery or failover: you have to plan it. Azure backup and disaster recovery explains the options.

First steps

1. Check Azure Service Health in the Azure portal. Microsoft says it gives a personalised view of the Azure services and regions you use, and Resource Health shows the state of an individual virtual machine.
2. If one virtual machine is affected, restore it from Azure Backup, following the steps in Backups.
3. If you replicate with Azure Site Recovery, follow your recovery plan to fail over to the secondary region, then fail back when the primary is running again. Microsoft says recovery plans let you set the order in which machines fail over.
4. Tell staff and customers which services are affected and when you expect them back.

What to record	Example	Yours
Who acts	[IT support provider], with [Name], IT lead	
Escalate when	[The server can't be restored within its RTO, or Microsoft reports a region-wide problem]	

g. A key supplier fails

> **How to fill it in:** Use this when a supplier you depend on, such as your IT support provider, a software company or a cloud service, stops providing its service. The NCSC advises planning for the sudden loss of a supplier's services and understanding the resilience arrangements of your key suppliers.

First steps

1. Find out what has stopped and for how long, using the numbers in Roles and contacts.
2. Switch to your workaround: a manual process, another supplier, or a system you already have.
3. Make sure you can still get your data: where it's held, and how you'd export it.
4. If the supplier has admin access to your systems and may have been attacked, review that access. The NCSC warns that attackers may target suppliers as a way into their customers.
5. Check the contract for notice periods, exit terms and how your data is returned.

What to record	Example	Yours
Who acts	[Name], Managing director, with the owner of the affected system	
Escalate when	[The supplier can't say when service will return, or a tier 1 system is affected]	

6. Testing log

How to fill it in: Record every test: what you tested, what happened and what you changed afterwards. The NCSC says plans should be tested regularly, with a full exercise where possible, because many plans fail in practice.

Testing log

Date	Test type	Scenario or system	Who took part	What happened	What we changed afterwards
[Date]	Tabletop exercise	Microsoft 365 outage	[Managing director, office manager, IT lead]	[We couldn't find staff mobile numbers without Outlook]	[Printed contact list added to the plan]
[Date]	Restore test	[Accounts server, from Azure Backup]	[IT support provider]	[Restored in [3 hours], within its RTO]	[None]
[Date]	Contact test	Reaching staff without email or Teams	[All staff]	[[18] of [20] replied within an hour]	[Two phone numbers updated]

7. After an incident

How to fill it in: After every incident, review what happened while it's fresh, and update the plan. The NCSC advises revising your incident plan with the lessons learnt, so the same thing can't happen in the same way again.

What to record	Example	Yours
Incident	[What happened, and any supplier or Microsoft incident ID]	
How long it affected us	[Start date and time] to [end date and time]	
Review held on, and who attended	[Date], [names or roles]	
What worked	[...]	
What didn't work	[...]	
Reports made	[NCSC, Report Fraud or Police Scotland, ICO, insurer, SLA claim], with reference numbers	

What to record	Example	Yours
Changes to the plan	[What changes, who does it, by when]	
Plan updated to version	[1.1], on [date]	

Questions to ask

- Did we know quickly that something was wrong, and who told us?
- Could we reach everyone we needed to?
- Were our RTOs and RPOs realistic?
- Did the backups restore, and how long did it take?
- What would we do differently next time?

> For a Microsoft incident, add Microsoft's post-incident report from Service health to your review. Service health keeps 30 days of history, so save a copy.

Appendix A. Microsoft's SLA

> **How to fill it in:** This explains where Microsoft publishes its service level agreement (SLA) and how to claim a service credit. It's a short summary of Microsoft's document: the SLA itself is what counts.

Where it's published. Microsoft publishes the Service Level Agreement for Microsoft Online Services, which covers Office 365, Azure, Dynamics 365 and Intune, on its licensing site: Service Level Agreements (SLA) for Online Services. The SLA says the current version is always at aka.ms/CSLA.

Which version applies. Microsoft says it won't change your SLA during the initial term of your subscription; when you renew, the version current at renewal applies for the whole renewal term.

What to record	Example	Yours
Our subscription renews on	[Date]	
Who submits a claim	[Name], or [our Microsoft licensing partner]	

What a credit is. If Microsoft doesn't meet a service level, you may be eligible for a credit towards part of your monthly fees for that service. Service credits are your sole and exclusive remedy, and Microsoft doesn't award them for lost revenue, operational costs or other losses.

How to claim. Submit the claim to Microsoft customer support with all the information Microsoft needs to check it. Microsoft rejects claims without the required information, which includes:

- a detailed description of the incident;
- the time and duration of the downtime;
- the names of the affected resources;
- the number and locations of affected users;
- a description of the errors.

When. For Microsoft 365 and other services apart from Azure, Microsoft must receive the claim by the end of the month after the month of the incident: for an incident on 15 February, by 31 March. Azure claims must reach Microsoft within 60 days of the incident. Microsoft says it typically processes claims within 45 days.

What isn't covered. The SLA doesn't apply to problems outside Microsoft's reasonable control, such as a network or device failure at your site or between your site and Microsoft's data centre, or to problems caused by not following appropriate security practices. Free services and previews aren't eligible.

> Each service has its own definition of downtime and its own credit levels in the SLA. Microsoft makes a good-faith decision on whether a credit is owed, from the information available to it, and you must be complying with your agreement to be eligible.

Appendix B. Example: scenario a filled in for the 12 November 2026 Microsoft 365 outage

This is scenario a, Microsoft 365 outage, filled in as a small business on Microsoft 365 might have recorded the outage that began on 12 November 2026. Microsoft's updates are summarised from its public status page and its Microsoft 365 Status account on X, in UK time (GMT). Entries in square brackets are the business's own, and are examples. Microsoft took the incident off its public status page at 05:42 on 14 November without saying there that it was resolved, so this example has no end time.

What to record	In this example
Incident	EX1550543, with MO1550821 (Microsoft's IDs in Service health)
What Microsoft said was affected	Exchange Online, and features of other Microsoft 365 services that depend on it. Users may be unable to reach their mailbox in Outlook on the web, Outlook desktop, Exchange ActiveSync or REST-based apps, and email delivery may be delayed.
What still worked, according to Microsoft	Most core Teams features, including calls, meetings, group chats and channel messages. Files stored directly in SharePoint Online could still be opened.
Cause, according to Microsoft	An issue introduced during an earlier network capacity upgrade, which surfaced after a recent network change. Microsoft said it was a technical issue, not related to cyber or AI.
Plan invoked	[18:10 on 12 November, by the managing director]

Timeline kept for the incident log and the SLA claim

UK time	What Microsoft said	What we did
17:54, 12 Nov	Investigating reports of users having issues accessing Exchange Online mailboxes through multiple connection methods in the Americas (EX1550543)	[Staff report that Outlook won't connect. IT lead checks Service health.]
18:07	The issue may affect users in any region	[Plan invoked. Group text to all staff: email is down, use Teams chat, next update by 20:00.]
18:35	Elevated load on part of its infrastructure across multiple regions; details under EX1550543 and MO1550821	[Turned on Manage notifications for this issue, including an address outside Microsoft 365.]
00:56, 13 Nov	Admins may be unable to load some admin centre pages; core Teams messaging and meetings remain largely working	[Noted for the morning: check status.cloud.microsoft if the admin centre won't load.]
09:10 to 10:01	Email timeout window extended to 48 hours, to preserve delayed messages	[Customers told by phone that emails may arrive late.]
12:00	Encouraging recovery progress in Europe	[Spot check: [3] of [12] staff can send and receive.]
17:57	Underlying issue addressed; a technical issue, not related to cyber or AI	[Staff update: service recovering, delayed email still arriving.]
20:02	Sign-in and access may recover before email delivery fully catches up	[Asked staff to report any email still missing.]
22:00	Sustained recovery; monitoring for an extended period, including the backlog of queued email, before considering it resolved	[Last report of a problem from our staff at [time].]

UK time	What Microsoft said	What we did
05:42, 14 Nov	Incident taken off Microsoft's public status page, without saying there that it was resolved	[IT lead checks Service health for Microsoft's latest update.]

What to record	In this example
Who acted	[Name], IT lead: Service health and Microsoft's updates. [Name], Office manager: staff and customer messages. [Name], Managing director: invoked the plan.
Workarounds used	[Outlook showed email already downloaded, and replies waited to be sent. Teams chat for internal messages. Files opened from SharePoint, and from OneDrive files kept on devices.]
Escalated	[09:00 on 13 November, past our 4-hour RTO for email: phoned our ten largest customers.]
SLA claim	Microsoft must receive any claim by 31 December 2026, the end of the month after the incident. [Evidence kept: this timeline, the number and locations of affected users, error messages and screenshots. Claim to be submitted by [Name].]
Lessons learned	[Our Service health emails went only to an Exchange Online mailbox we couldn't open. We added an address outside Microsoft 365, and a printed staff phone list.]

> For incidents with broad impact on many organisations, Microsoft says it delivers a preliminary post-incident review in Service health within 48 hours of the incident being resolved, and a final one within five business days. Add it to your after-incident review.