

IT Disaster Recovery Plan Example

IT Disaster Recovery Plan Example

An IT Disaster Recovery Plan explains how an organisation will recover its technology, applications and data following an IT incident.

This example demonstrates how a small UK business could document recovery procedures for Microsoft 365 servers, backups, internet connectivity, cyberattacks and ransomware.

The example is fictional. Should be adapted to the organisations own IT environment.

IT Environment Example

A small UK business may depend on:

- ⑩ Microsoft 365
- ⑩ Email and calendars
- ⑩ file storage
- ⑩ Business applications
- ⑩ Accounting software
- ⑩ CRM
- ⑩ Network infrastructure
- ⑩ Internet connectivity
- ⑩ Employee laptops
- ⑩ Servers or hosted infrastructure
- ⑩ Backup systems

Each critical system should have a documented recovery procedure.

1. Microsoft 365 Recovery

Microsoft 365 may be essential for email, calendars, collaboration and access to business information.

The IT Disaster Recovery Plan should identify:

- ⑩ Microsoft 365 services used by the organisation
- ⑩ Who administers the environment
- ⑩ Who provides support
- ⑩ How important business data is protected
- ⑩ What alternative communication methods are available
- ⑩ What the organisation will do during a service outage

How recovery responsibilities are assigned

The organisation should also document support and escalation procedures.

2. Server Recovery

For each server or hosted system, document:

- ⑩ Server name
- ⑩ Server purpose
- ⑩ Applications hosted on the server
- ⑩ Location or hosting provider
- ⑩ arrangements
- ⑩ Recovery priority
- ⑩ Recovery procedure
- ⑩ Responsible person
- ⑩ External IT provider details
- ⑩ System dependencies

The recovery procedure should contain information, for the responsible IT team or provider to understand what needs to be restored.

3. Backup and Data Recovery

A reliable backup strategy is a part of disaster recovery.

The IT Disaster Recovery Plan should document:

Backup Frequency:

- ⑩ Record how critical systems and data are backed up.

Backup Location:

- ⑩ Record where backups are stored and whether alternative or off-site storage is used.

Backup Retention:

- ⑩ Document how long different backup copies are retained.

Backup Protection:

- ⑩ Document how backups are protected from access, accidental deletion and incidents that could affect the primary environment.

Restoration Testing:

- ⑩ Backups should be tested through restoration checks to confirm that data can actually be recovered.

A successful backup job does not by itself prove that recovery will work.

4. Internet Failure

Internet access might be very important for cloud programs Microsoft 365 and for talking with people.

If the main internet connection stops working the recovery process should have these steps:

- ⑩ Check if there is a problem with the internet.
- ⑩ Look to see if the problem is affecting everyone in the company or a few people.
- ⑩ Call the company that provides the internet service.
- ⑩ Write down when the internet is expected to come
- ⑩ Use another internet connection if that is possible.
- ⑩ Make sure the important people and computers get help first.
- ⑩ Tell the workers about the effect the problem is having.
- ⑩ Keep watching the situation until the internet is working again.

The real plan must have the contact information for the internet service provider.

5. Cyberattack Recovery

If someone thinks there is a cyberattack the company should follow its written steps for dealing with incidents and getting back to normal.

The recovery process should have these steps:

- ⑩ Find out what the possible problem is.
- ⑩ Take the computers that are affected out of the network if that is needed.
- ⑩ Tell the person who's in charge of handling the incident.
- ⑩ Call the IT company or the people in the company who handle IT.
- ⑩ Check which computers and data are affected.
- ⑩ Keep the computers that are not affected safe and use the backups that're available.
- ⑩ Find the points to get back, to.
- ⑩ Get the important computers working again based on what is most needed.
- ⑩ Test the computers that is back up and running.

Write down what happened and check the recovery process after.

6. Ransomware Recovery

Ransomware can stop people from using their computers and data. Should be thought about when making an IT Disaster Recovery Plan.

The plan should explain how the company will:

- ⑩ Find out which computers are affected
- ⑩ Take the devices that are affected out of the network
- ⑩ Tell the people about the problem
- ⑩ Keep the computers that are not affected safe

- ⑩ Keep the backups and other recovery tools safe
- ⑩ Find the best points to get back to
- ⑩ Bring the most important computers back up
- ⑩ Check the data that is back
- ⑩ Tell people about the recovery process
- ⑩ Look at what happened after everything is fixed

The exact way to fix the problem will depend on the company IT setup.

7. Recovery Priorities

Critical systems should be assigned recovery priorities.

IT System	Priority	Example RTO
Email	High	4 hours
File Storage	High	4 hours
Accounting	High	8 hours
CRM	Medium	24 hours
Individual Devices	Medium	24-48 hours

These are example targets only. Each organisation should establish recovery targets based on its own operational requirements.

8. RTO and RPO

Recovery Time Objective (RTO)

- ⑩ RTO is the time limit within which a system must be up after an incident happens.
- ⑩ For example a company might set an RTO of four hours for its email service. That means the email system should be working again within four hours after the disruption.

Recovery Point Objective (RPO)

- ⑩ RPO shows how data loss the organisation is willing to accept.
- ⑩ For instance an RPO of 24 hours means the recovery process needs to restore data that's no older than one day.
- ⑩ This helps decide how often backups should run.

Both RTO and RPO need to be written down for every important system in the business.

Having these targets helps teams act quickly and effectively during an emergency.

9. IT Recovery Team

The IT recovery team should consist of roles such as:

- ⑩ Incident Lead

- ⑩ IT Recovery Lead
- ⑩ Internal IT Administrator
- ⑩ Operations Manager
- ⑩ Communications Lead
- ⑩ External IT Provider

Each person on the team has specific duties during a crisis.

It's very important to define these responsibilities before any incident occurs.

Clear roles prevent confusion. Improve response speed.

10. After Recovery

Once systems have been restored the organisation must take the following steps:

- ⑩ Confirm that critical systems are working properly.
- ⑩ Check that all restored data is available and accurate.
- ⑩ Make sure users can access the services they need.
- ⑩ Keep an eye on systems for any issues.
- ⑩ Record every action taken during the recovery process.
- ⑩ Review whether the original RTOs and RPOs were met.
- ⑩ Note what went well and what could be improved.
- ⑩ Update the Disaster Recovery Plan based on lessons learned.

Need a Complete Disaster Recovery Plan?

This page gives an IT-focused example.

For a disaster recovery plan suitable for small to medium-sized businesses, including editable templates and structure visit:

[Disaster Recovery Plan Template for SMEs, →]