

Disaster Recovery Plan Example for UK SMEs

A Disaster Recovery Plan or DRP must give easy-to-follow steps for getting an organisation's IT systems and data back up and running after a major disruption. This example outlines how a small business, in the UK might set up a Disaster Recovery Plan. It is not real—it is fictional. Each business must change this plan to fit its systems, risks, people and recovery needs.

Example Business

- **Business:** Example UK Professional Services Ltd
- **Employees:** 25
- **Location:** United Kingdom
- **Business type:** services

Critical IT Systems

The business depends on these systems every day to work properly:

- Microsoft 365
- Email and calendars
- Cloud file storage
- Accounting software
- Customer Relationship Management (CRM) system
- Internet connectivity
- Employee laptops and desktop computers

These systems are essential. If any of them fail the business could not operate normally. A good disaster recovery plan starts by identifying which systems matter most. Then it outlines how to restore them quickly as possible.

1. Recovery Priorities

Not every system needs to be recovered at the time. The business should figure out which systems are most important and bring them back based on how they affect the business.

System	Priority	Target Recovery Time	Business Impact
Microsoft 365 Email	High	4 hours	Staff communication affected
File Storage	High	4 hours	Staff unable to access documents
Accounting System	High	8 hours	Finance operations affected
CRM	Medium	24 hours	Sales activity delayed
User Devices	Medium	24–48 hours	Individual staff affected

These recovery targets should be reviewed regularly and changed when business requirements change.

2. Example Disaster Scenario: Ransomware Attack

Imagine that several employee computers get infected with ransomware and files can't be opened any more.

The organisation should follow its written rules for handling incidents and recovery.

Initial Response

1. Find out which devices and systems are affected.
2. Separate the affected devices or systems if needed.
3. Tell the person who handles incidents.
4. Get in touch with the IT team or an outside IT company.
5. Check which systems and data might have been hurt.
6. Keep the systems that are not affected safe and protect the backups that're still there.
7. Find points to restore from.
8. Start bringing back the important systems according to the plan.

Recovery

Once the affected area has been checked out the recovery team should:

- Bring systems back using proven recovery steps.
- Get data back from backups.
- Test the systems that are brought back before putting them into regular use.
- Make sure that important applications are working.
- Check that users can get to the systems they need.
- Keep an eye on the systems after recovery.

The incident should be written down. The Disaster Recovery Plan should be looked at again to find ways to get better.

3. Example Backup Strategy

The organisation should write down its backup plan clearly.

The plan should include:

- Which systems and data are backed up
- How often backups are done
- Where the backups are kept
- How long the backups are kept
- How the backups are kept safe
- Who watches the activity

- Who is in charge of bringing things back
- How testing, for restoration is done

Backups should be tested often to make sure the organisation can really get its data back when it needs to.

4. Example Communication Process

During a disruption employees should know:

- Who to inform about the incident
- How updates will be provided
- Which systems to stop using
- What other ways to communicate exist
- When normal work can be resumed

The organisation must also plan how to inform customers, suppliers and other important parties when needed.

5. Example Internet Failure Scenario

If the organisation loses its internet connection the recovery process could include:

- Check that the issue is not only on one device
- Reach out, to the internet service provider
- Ask for the expected time to restore service
- Use a backup connection if it is suitable
- Prioritise users and systems that need the internet for essential work
- Keep monitoring until normal internet returns

The actual plan should contain the relevant supplier contact details and escalation procedures.

6. Example Plan Review

After an incident or recovery test the organisation should review:

- What happened
- What worked well
- What did not work
- Whether the recovery goals were met
- Whether backups existed
- Whether staff knew their duties
- What improvements are needed

The Disaster Recovery Plan must then be updated where needed.

Need a Disaster Recovery Plan Template?

This example shows how a finished recovery plan might look. To create your plan use our Disaster Recovery Plan Template for SMEs.

[\[View the Disaster Recovery Plan Template →\]](#)