

Disaster Recovery Testing Checklist

A Disaster Recovery Plan should be tested regularly to confirm that recovery procedures work as expected.

A Disaster Recovery Plan may look complete on paper. Testing can uncover missing information, outdated contact details, unavailable backups or recovery procedures that do not work as expected.

Use this Disaster Recovery Testing Checklist to review your organisations recovery arrangements.

1. Disaster Recovery Plan Review

- ☐ Confirm that the current Disaster Recovery Plan is available to the people.
- ☐ Check that the Disaster Recovery Plan has a version number.
- ☐ Check the updated date of the Disaster Recovery Plan.
- ☐ Check the review date for the Disaster Recovery Plan.
- ☐ Confirm that critical systems are still included in the Disaster Recovery Plan.
- ☐ Confirm that recovery priorities in the Disaster Recovery Plan are still accurate.
- ☐ Confirm that RTOs and RPOs in the Disaster Recovery Plan are still appropriate.
- ☐ Update the Disaster Recovery Plan if the organisations systems or processes have changed.

2. Critical Systems Checklist

- ☐ Microsoft 365 services documented.
- ☐ Email system documented.
- ☐ File storage documented.
- ☐ Accounting software documented.
- ☐ CRM documented.
- ☐ Internet connectivity documented.
- ☐ Servers documented.
- ☐ Critical applications documented.
- ☐ Important dependencies documented.

3. Backup Testing Checklist

- ☐ Confirm that scheduled backups are running.
- ☐ Check backup results.
- ☐ Confirm that critical data is included in backups.
- ☐ Confirm that backup locations are documented.
- ☐ Confirm that backup retention is documented.
- ☐ Check that backups are appropriately protected.
- ☐ Perform a test restoration.

- Confirm that restored files can be. Used.
- Record the results of restoration testing.
- Resolve any backup failures.

4. Ransomware Recovery Test

- Select a ransomware scenario.
- Identify which systems could be affected by ransomware.
- Confirm who should be notified in a ransomware event.
- Confirm how affected systems would be isolated.
- Confirm that recovery resources are available for ransomware.
- Identify a recovery point, for ransomware.
- Test the documented recovery process where appropriate.
- Confirm that restored systems can be tested before use.
- Record problems discovered during the ransomware exercise.

5. Microsoft 365 Recovery Review

- Check that the responsibilities for Microsoft 365 are written down.
- Check that the administrator or support contacts are up to date.
- Check that ways to communicate are written down.
- Look at the plans for getting business data back.
- Check that the steps to take if things go wrong are available.

6. Server Recovery Test

- Check that the server information is up to date.
- Check the priorities for recovering the server.
- Check the backup plans are in place.
- Look at the written steps for recovery.
- Check that the technical contacts are known.
- Test the steps to restore the server where needed.
- Write down what happened during the test.

7. Internet Failure Test

- Check the contact details for the internet provider.
- Look at the steps to take if there is a problem.
- Check if there is another way to connect to the internet.

- ☐ Find out which systems need the internet to work.
- ☐ Check how employees will do their work if the internet is down.
- ☐ Write down any issues found during the test.

8. Incident Response Test

- ☐ Check that employees know how to report an issue.
- ☐ Check who is in charge of handling the incident.
- ☐ Check who is in charge of getting IT up.
- ☐ Check who is responsible for communication.
- ☐ Check the details for any IT help.
- ☐ Check the contact details for suppliers.
- ☐ Test the way people communicate during a problem.

9. Communication Test

- ☐ Check how employees will get updates.
- ☐ Check how customers will be told if needed.
- ☐ Check how suppliers will be told if needed.
- ☐ Check ways to communicate.
- ☐ Check who is allowed to speak to people, outside the company.

10. Record the Test Results

Every Disaster Recovery test should be documented.

Date of test: _____

Scenario tested: _____

Systems tested: _____

People involved: _____

After the Test

Testing is only useful if the results are acted upon.

After each test:

- ☐ Review the test results.
- ☐ Assign responsibility for identified actions.
- ☐ Resolve backup or recovery problems.
- ☐ Update contact information.
- ☐ Update recovery procedures where required.

- Update. Rpos if business requirements have changed.
- Update the Disaster Recovery Plan.
- Record the date of the review.

Need a Disaster Recovery Plan?

Testing is one part of effective disaster recovery.

If you need to create or improve your organisations plan see our:

[Disaster Recovery Plan Template for SMEs, →]