

SMALL & MEDIUM BUSINESS

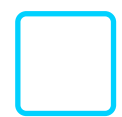
IT DISASTER RECOVERY PLANNING

CHECKLIST

Our IT Disaster Recovery Planning Checklist

Disaster Recovery Plans can support business continuity as it focuses on recovering critical information technology after a disaster to ensure business functions resume within an acceptable amount of time. As a proactive CEO, you know implementing a disaster recovery plan is essential for your business and the key is to **start** a plan and improve it over time.

Below we provide a checklist of items to consider for your own Disaster Recovery Plan.



Determine the acceptable amount of down time.

This identifies your Recovery Time Objective (RTO) which is the amount of downtime that can pass between a disaster and recovery of normal business operations.

Ask yourself:

- How long can I wait until my business applications and services are restored? 30 minutes? 2 hours? 6 hours? 24 hours?
- What am I willing to spend to minimize my downtime?
- Note: Your RTO may vary with each application. This is where prioritizing is helpful to determine which one needs recovery first.



Determine how much data you can afford to lose.

This identifies your Recovery Point Objective (RPO) which is the maximum amount of data loss when a disaster occurs. This is a helpful variable to determine how often you should backup your data.

Ask yourself what you are willing to lose:

- 1 hour of email communication?
- 3 hours of accounting data?
- 6 hours of file changes?
- 24 hours of your business application data?

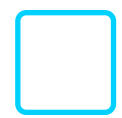


Determine where employees will work if the physical building is not accessible.

Building closure can be due to fire, flood, etc. It is important to determine where staff are going to work if they cannot access the building.

Ask yourself:

- How will my customers contact me?
- Would another location be required?
- Could everyone work from home?
- Which staff require remote access?
- How can my team communicate with each other?



Document all hardware and software.

Understanding the impact of a disaster on your business requires a full understanding of the organizations systems and assets. Document all critical infrastructure and software licensing including both physical and Cloud based. In the event of a total loss, consider exactly what items are needed to bring your business back to normal operations.

Consider documenting the following:

- Purchase date, serial number, version, and vendor information.



Identify what business applications and services require internet connection.

If you are hosting critical internal services like company webpages, your business ERP/CRM or email, ensure that there is redundant internet connection. If these services are considered critical to your business, you may want to think about moving them to the Cloud to lower your risk.



Document the process.

Document every defined process around recovery on paper, assign teams to each step in the process, make all team members aware of their roles and distribute copies of the process to every team member, as well as keeping copies somewhere secure offsite.



Test the process!

Choose a safe moment in time that allows you and the teams who are involved to test the Disaster Recovery Plan. You will be able to uncover any unforeseen issues that only become visible when theoretical situations become reality, along with creating some mental muscle memory on how to go about the process when an event occurs. Weed these out and be prepared before an outage happens at an unplanned time.

- Note: No plan is perfect at the beginning. After testing, remember to make the changes and adjustments necessary for the plan.

Having a Disaster Recovery Plan in place for your business is necessary for business continuity.

Identifying and applying important variables like Recovery Time Objective and Recovery Point Objective to your Disaster Recovery Plan can help minimize the level of disruption to your business.

Now that you have completed the checklist, you are on the path to being well prepared if a disaster ever strikes.

