

Disaster Planning Checklist

Assessing Your Risk:

- Define all critical functions, systems, software and data in your organization.
- Prioritize the above items in order of importance to your business (mission critical to minor) based on which ones, if destroyed or impacted by change, would have the greatest negative impact on your business.
- Create a document that outlines your current IT infrastructure (network documentation) so that it is readily available should recovery or modifications need to be made.
- Determine the RTO (recovery time objective), RPO (recover point objective) and MTO (maximum tolerable outage) for every critical function and system in your business.
- Identify all threats that could potentially disrupt or destroy the above-mentioned data, systems, functions, etc. and the likelihood of those threats.

Mitigation and Planning Strategies:

- Create an IT Assets Inventory list and identify all the functions, data, hardware and systems in your business.
- For each mission-critical system or function, document ways to minimize, avoid or limit the damage done.
- Create a disaster recovery plan specific to what damage could be done (tornado flattens your office, city evacuation, virus attack, etc.), and identify who will be responsible for executing the plan (your disaster recovery team).
- Identify a recovery plan and timeline for each function, and prioritize these functions by the order in which they need to be recovered if multiple mission-critical functions were affected.
- Create a backup strategy for your data and systems.
- Create a testing and validation strategy, and schedule tests for your backups.
- Define your communication plan in the event of a disaster to employees, clients, vendors and the media.
- Create a “break the glass” document that contains instructions on what to do if a key executive dies, is disabled or is otherwise unavailable for a long period of time.
- Review your current insurance policy to make sure you have sufficient coverage to replace the assets (including data that has been compromised) in your organization.
- If applicable, define a media communication strategy (how you will communicate with the press if a disaster happens). Some industries have requirements.
- Summarize this into a disaster recovery plan and brief the disaster recovery team on the plan.
- Schedule a periodic review and update the plan with your disaster recovery team.

Important: This checklist should only be used as a starting point for your Disaster Recovery Plan. This is in no way complete; we highly recommend you engage with a professional IT firm to map out a complete Disaster Recovery Plan for your business.

[Click here to visit our website to learn more about Disaster Recovery or contact us.](#)