Disaster Planning Checklist

This template is a starting point for a Disaster Recovery Plan. Without knowledge of your specific business, operations and risks it is impossible to draft a policy that covers all aspects.

Provided By:
Steven Lauber
Trailhead Networks
1000 Front Ave NW
Grand Rapids, MI 49504
www.trailheadnetworks.com

Follow me on social media

Disaster Planning Checklist

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.

Risk Assessment:

- ❑ 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, would have the greatest negative impact on your business.
- ❑ Create a document that outlines your current IT infrastructure (network documentation) so another IT person or company could take over easily if your current IT person wasn't available, or could assist in the recovery of your IT infrastructure in the event of a disaster.
- ❑ 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.
- ❑ Identify all potential disasters and threats to these systems and functions.
- ❑ For each mission-critical system or function, brainstorm ways to minimize, avoid or limit the damage done.
- ❑ For the most likely disasters, 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 in your organization.

- ❑ Define a media communication strategy (how you will communicate with the press if a disaster happens).
- ❑ Summarize this into a disaster recovery plan and brief the disaster recovery team on the plan.
- ❑ Schedule a periodic meeting to review and update the plan with your disaster recovery team.