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.

There are many types of disasters, and your DR plans need to account for different situations. For example, a natural disaster (fire, flood, tornado, hurricane) is different than a hardware failure on your server(s), which is also different than a cyber-attack or ransomware event, which is different than a key person in your company passing away.

Ensure your DR plans account for the various types of events that your business would classify as a disaster.

Risk Assessment:

- ❑ Define all critical functions, systems, software and data in your organization.
  - Line of Business applications
  - Key functions or services your company provides and how it generates revenue
  - CRM or other customer management system
  - Critical data and files, such as accounting, customer information, financial, document management system, HR, tax records, etc.

- ❑ 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. Detail what systems or data needs to be restored or accessible first, second, third, etc.

- ❑ Create a document that details and outlines every single thing in your current IT infrastructure (network documentation) so your staff, 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. Don't forget to have a good Password Management and Documentation system in place so they can actually perform the steps needed. Your IT provider should be able to easily generate this for you.

- ❑ 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. Again, your IT provider should be able to generate this for you at any time.

- ❑ Identify all potential disasters and threats to these systems and functions. Create a disaster recovery plan specific to what damage could be done (tornado flattens your office, fire, flood, cyber-attack, etc.), and identify who will be responsible for executing the plan (your disaster recovery team).

- ❑ For each mission-critical system or function, brainstorm ways to minimize, avoid or limit the damage done. Implement redundancy where it is deemed necessary.

- ❑ 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 regular tests for all of your backups. The time to determine your data backups are not recoverable is not when you need to recover the data. We have seen this happen too many times!

- ❑ 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, cover business interruptions, provide cyber protection coverage, pay for restoring systems and data, etc.

- ❑ Summarize this into a disaster recovery plan and brief the disaster recovery team on the plan. Have written step by step instructions on the process.

- ❑ Schedule a periodic meeting (at least annually) to review and update the plan with your disaster recovery team.