SYSCON

Syscon's Disaster Planning Checklist

Providing technology solutions

This checklist should only be used as a starting point for your Disaster Recovery Plan. This is in no way complete; we highly recommend that you engage with a professional IT firm to map out a complete Disaster Recovery Plan for your business. We're happy to help–call us at 630-850-9039.

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 can easily take over if your current IT person isn't available or can assist in the recovery of your IT infrastructure in the event of a disaster.

☐ Determine the Recovery Time Objective (RTO), the Recover Point Objective (RPO) and Maximum Tolerable Outage (MTO) for every critical function and system in your business.

☐ Identify all threats that could potentially disrupt or destroy the above mentioned data, system 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 damage done.

☐ For the most likely disasters, create a recovery plan specific to what damage could be done (tornado flattens your office, city evacuation, virus attack, etc.) and identify who is responsible for executing the plan (your disaster recovery team).

☐ Identify a recovery plan and timeline for each function, and prioritize these by the order in which they need to be recovered if multiple mission-critical functions are 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 with 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 ensure you have sufficient coverage to replace your organization's assets.

☐ Summarize all these items into a disaster recovery plan and brief the disaster recovery team on the plan.

☐ Schedule a periodic meeting to review and update your plan with your disaster recovery team.