A BUSINESS PREPAREDNESS GUIDE FOR TECHNOLOGY CONTINUITY

Step-by-Step Procedures to Prepare for the Worst

When it comes to disaster preparedness for your business, you must prepare for the worst.

When an incident, whether internal or external, manmade or natural, negatively affects your IT infrastructure, your business could be compromised.

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.

This guide is intended to provide the basics you need to develop an IT disaster and recovery plan. These step-by-step procedures will ensure you can recover disrupted systems and networks, so you can resume normal operations after a disaster.

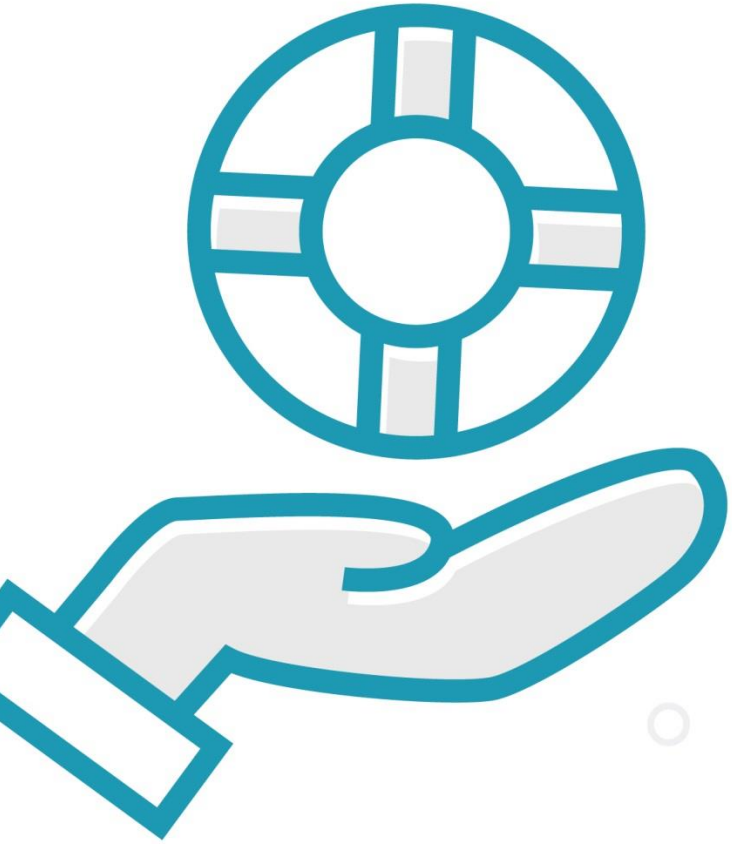
THE STEPS IN THIS eBook SHOULD BE MODIFIED AS NEEDED TO ACCOMPLISH YOUR GOALS.

Note: It's assumed that you've maintained continuous, off-site backups of data, applications, and server images. With offsite backups to the cloud, even the smallest company can ensure it is ready in the event of a disaster. Ensure your IT Professional has implemented the following:

- A System-Wide Data Backup
- Fully managed Backup and Disaster Recovery solutions that support multiple vendors and sites
- Appropriate Bandwidth to optimize backups
- Data Recovery with physical and virtual data storage.
- Proactive and preventive maintenance, monitoring, updates and patch management
- Connectivity between multiple data centers
- Secure IT environments from end to end

PREPARE A CONTINGENCY POLICY STATEMENT.

This is a formal policy that designates the authority and guidance to develop an effective contingency plan. Your executive team should meet with the internal or external technology team, to establish the scope of the activity to include in your plan. Gather all relevant network infrastructure documents, such as network diagrams, equipment configurations, databases. Obtain copies of existing IT and network plans.



CONDUCT A BUSINESS IMPACT ANALYSIS (BIA).

This is done to identify critical IT systems and components, and prioritize their recovery-time objective. It should predict the consequences of disruption and contain information needed to develop recovery strategies. Potential loss should be identified and quantified. Identifying and evaluating the impact of a disaster on a business provides the basis for investment in recovery strategies, prevention and mitigation strategies. The BIA report should prioritize the order of events for restoration of the business. Business processes with the greatest operational and financial impacts should be restored first.

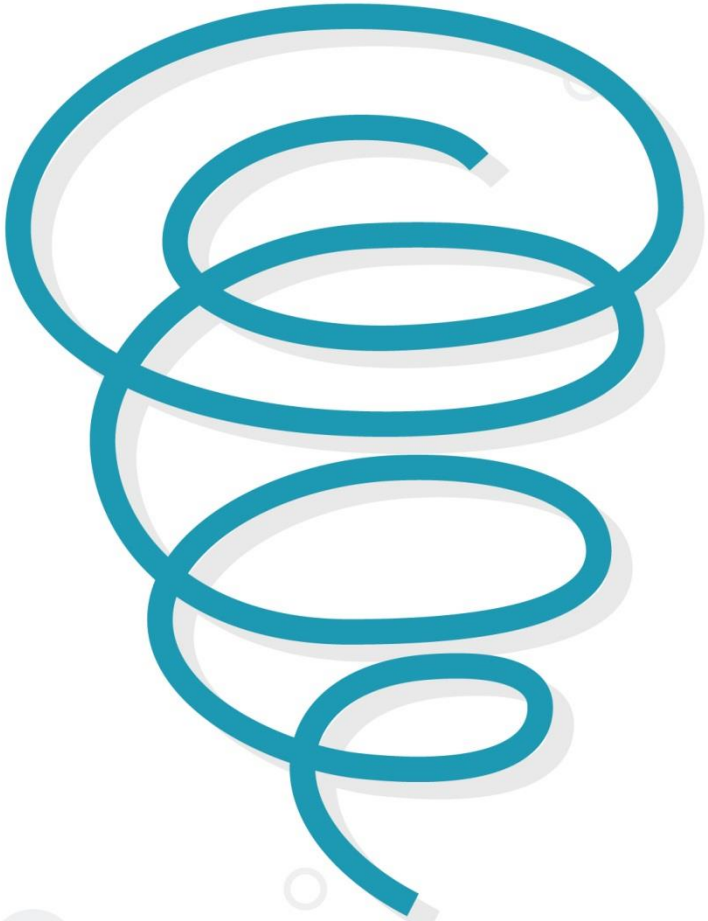
IDENTIFY PREVENTIVE MEASURES.

These are controls to reduce the effects of system downtime and can help to increase IT system availability. Installation of antivirus and anti-spyware software and maintaining strong firewalls are essential to protect network and information security. Keeping computers updated with the latest operating system and application “patches” should be part of any disaster preparedness program.

Information technology includes many components such as networks, servers, desktop and laptop computers and wireless devices. The ability to run both productivity and enterprise software is critical.

ESTABLISH EMERGENCY RESPONSE TEAMS for all critical IT infrastructure disruptions; determine their level of training with critical systems, especially in emergencies.

Additionally, identify vendor emergency response capabilities; if they have ever been used; if they were working properly; how much you are paying for these services; the status of service contracts; and the presence of service-level agreements (SLA).



DEVELOP RECOVERY STRATEGIES FOR INFORMATION TECHNOLOGY.

Technology must be restored in time to meet the needs of the business. Manual workarounds should be part of the IT plan so business can continue while computer systems are being restored.

An information technology disaster recovery plan should be developed in conjunction with a business continuity plan. Priorities and recovery time objectives for information technology should have been developed during the business impact analysis (BIA). Strategies should be developed to restore a damaged network, including hardware, applications and data in time to meet the needs of the business recovery.

TRAIN, TEST AND PRACTICE TEST THE PLAN

to identify weakness and gaps. Compile results from assessments into a gap analysis report that identifies what is currently done versus what ought to be done. Include recommendations as to how to achieve the required level of preparedness, and estimated investment required. Once your preparations are in place, and you've set up the necessary objectives, you then can execute your test.

Train personnel in the steps they should take to activate the plan. A disaster recovery test involves:

- Dissemination of information regarding the disaster
- Implementation of recovery activity
- Monitoring processes
- Documentation of work performed
- Problems encountered
- Documentation of the results

Practice these steps regularly to improve plan effectiveness and overall preparedness.

UPDATE THE PLAN AS REQUIRED.

The plan should be fluid, not static, and updated regularly to remain current with business and network changes. Update The Plan documentation to reflect changes.

Considering the investments your business has likely made in your IT infrastructure, you should invest sufficient time and resources to protect those investments from unplanned and potentially destructive events.

PEGAS
TECHNOLOGY SOLUTIONS LLC

If you need help to develop a Disaster Preparedness Plan for your business, contact the experts at Pegas Technology Solutions. We'll ensure your technology and business are prepared for any disaster.

Email: sales@pegas.io On the Web: pegas.io