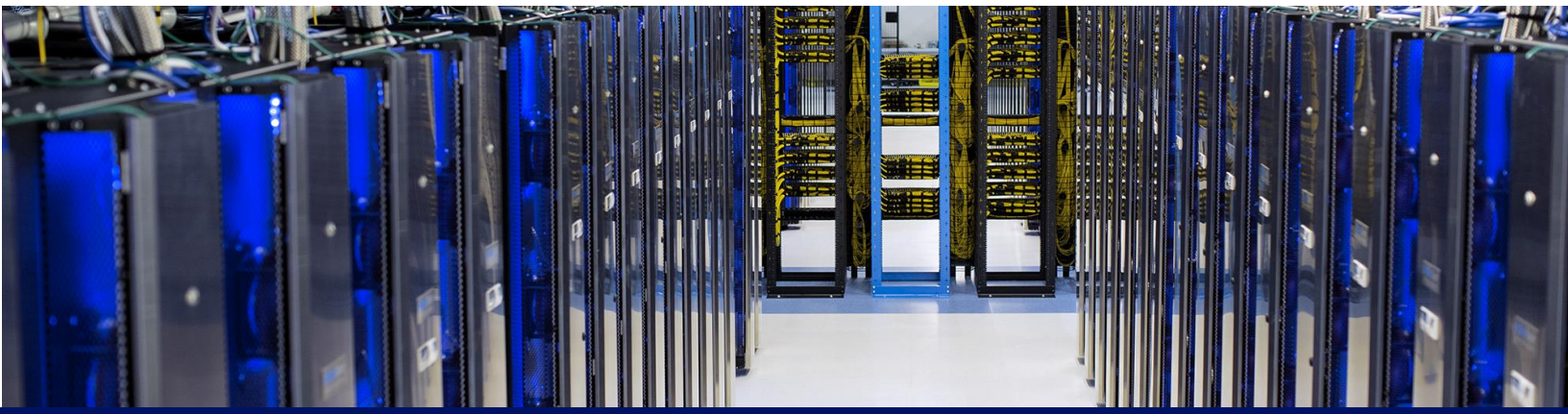
Microsoft



Disaster Preparedness **Technology Plan**

Use the cloud for anything you can

Many businesses keep critical servers, systems, and data on-site. That may make it easier for your IT team to service and maintain those important systems, but it can spell doom if your office takes on damage from a natural disaster. Cloud storage and web applications ensure that your important data and processes are always available, no matter what happens. They're also incredibly convenient for the mobile workforce.

Eighty percent of Fortune 500 companies use Microsoft Cloud, and with good reason – it provides accessibility to applications, data and processes, anywhere, anytime. This enterprise-grade technology is available to the smallest of businesses.

Back everything up, everywhere

Cloud services should also be used to create regular, redundant data backups in case your systems are damaged or compromised by a security threat. Don't limit your backups to just the obvious stuff. If your company uses smartphones and mobile applications as part of its workflow, make sure the data on those devices is also backed up. In addition to using cloud storage, it's wise to create hard-drive backups in case the online service you use is compromised or temporarily inaccessible.

Secure all your backups

You should apply the same security practices to your backups as you do with all your business data. That means encrypting all your files, whether they're online or on a hard drive. Otherwise, one stolen drive or password could put all your company's critical data in the wrong hands. And of course, please don't use passwords that are ridiculously easy to guess.

Azure Security Center offers protection against several kinds of cloud-based attacks, helping your data stay secure.

Disaster Preparedness **Technology Plan**

Ensure your tech is safe

An out-of-date operating system (OS) or unpatched software can be rife with security holes. To avoid exploits, make sure your software and OS are set up to install all the latest updates. They should include all the necessary security patches and other critical updates, and you can configure your PC to install them automatically. In Windows 10, automatic updates are enabled by default.

Each month, Microsoft releases a Windows Update to ensure the operating system is protected against the latest known vulnerabilities.

Keep important documents offline

Even if you have a well-thought-out plan, a disaster may make it inaccessible if it's stored on a computer. Make sure you have printed-out versions of your emergency contact lists, employee roles, and disaster-response plans and that they're easily accessible for your entire team. It's also a good idea to create a map of your systems architecture in the event your IT team cannot be on site. At least two people should be trained to do every disaster-recovery task.

When in doubt, ask for help

Even when there isn't a disaster to contend with, running a small- or medium-sized business can be a handful! If you need access to an IT expert that can ensure your disaster-response plan is built for success, the Microsoft Partner program is an invaluable resource. Ensure you have all the bases covered by visiting the Azure disaster-recovery guidance page, the Azure backup and archive website, and our guide to mitigating cybersecurity risks.

If your small business needs help with security and disaster recovery, a Microsoft Partner can help.

Microsoft