



DATA BACKUP

PROTECTING YOUR MOST VALUABLE ASSET

YOUR DATA IS HIGHLY VULNERABLE TO LOSS

As extraordinary and reliable technology has become over the years, it is by no means foolproof. Perhaps even scarier is the high probability that you could encounter any number of these various threats to your data at least once.



PHYSICAL SYSTEM FAILURES

Hard drive failure, software crashes or corruption.

EXTERNAL THREATS

Cyberattacks and hackers, malware, viruses and ransomware.

LOST/DAMAGED DEVICES

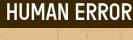
Device damage or loss due to intentional or unintentional causes, as well as natural disasters.

NATURAL & LOCAL DISASTERS

Fires, floods, power surges, and rodent or construction damage.

INSIDER THREATS

Employees who are disgruntled or have malicious intent.



User mistakes or unintentional errors.



WHAT DATA NEEDS BACKUP?

The simple answer is ALL DATA. Including all data and information assets in your backup process is a data protection best practice. Some data, if lost, may have a significant impact on your business, so it's crucial to identify all business-critical data by performing a risk and business impact assessment that includes the following questions:

Is the data personally identifiable, thereby requiring privacy? Is the data sensitive or potentially harmful in any way? Is the data irreplaceable or proprietary to the business?

HOW OFTEN DO I NEED TO BACK UP?

You'll want to configure your backups to fit your specific business.

A good way to start is by automating a daily backup of all the activities or transactions that take place each day. In addition, you should configure a minimum of one full image backup of all systems once every week.

WHAT BACKUP TYPES SHOULD I INCLUDE? There are three main types of backup approaches you should include as

part of your backup and disaster recovery plans.



regardless of any previous backups or circumstances.



alterations to the data set after the most recent full backup.



Only additions or changes taken place after the last/ most recent incremental backup.

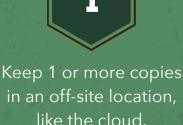
The 3-2-1 backup method is a best practice for protecting your data.

WHERE SHOULD MY BACKUPS BE STORED?





storage types.



TEST YOUR BACKUPS REGULARLY Check and test all your backups at least once per quarter. This frequency will

quantities of data assets. Regular testing is the only Check your backups routinely for way to monitor the success proper configuration and automation

likely increase if your business has very high data entry change rates or large

rates of backups and verify your data's integrity.

rapidly or have a high turnover. Testing ensures your business has the proper tools and right infrastructure needed to store and recover its critical data during and after any situation.

rules, especially if you are growing

Data is the lifeblood of your business and one of the most valuable assets you can acquire and possess. Proactive prevention is always better and less

REGULAR TESTING IS INSURANCE FOR YOUR BACKUPS Make routine testing a standard process of your backup and disaster

recovery strategy because it protects

your data, your reputation and your costly than a cure. long-term business success. If you need support implementing a comprehensive data backup and protection

CONTACT US TODAY TO SCHEDULE A CONSULTATION.

solution or want to ensure your current solution is up to the task, we can help.



sales@pcnetinc.com 2026 E Phelps St. Springfield, MO 65802