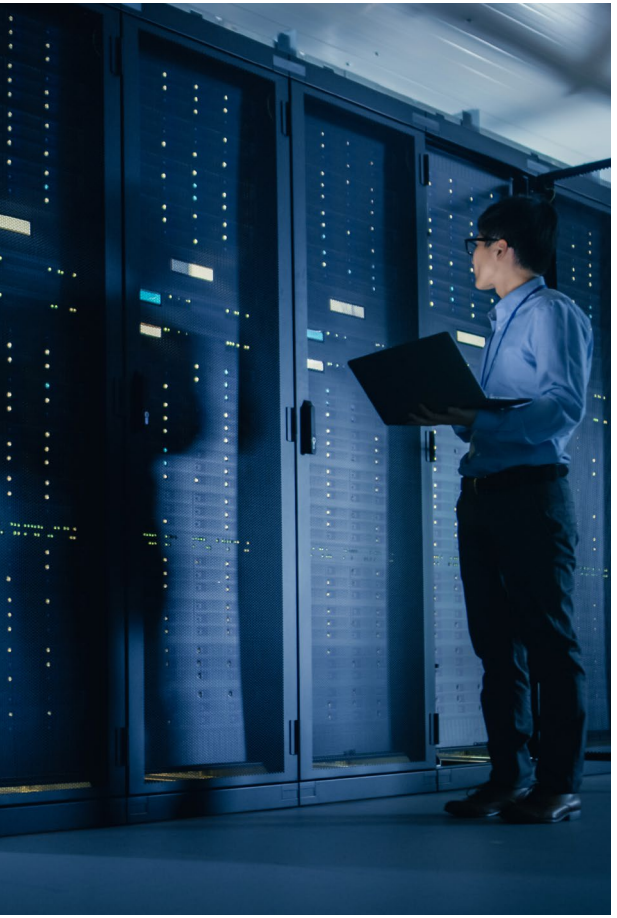
Cyber tips: Backup policies

VICTOR



Data is the most valuable part of a computer system and may be irreplaceable if lost to a ransomware attack or a hardware failure, or if it becomes corrupted. The following tips will assist you in planning and preparing a backup policy for an incident in case the worst happens.

What is a backup policy?

A backup policy is a well-thought-out plan to mitigate against data loss that could happen due to a ransomware attack, hardware failure, data corruption or some other detrimental event. If implemented well, it can help an organization return to business as usual more quickly and easily.

The complexity of the backup policy will depend on the size of the organization, the number of applications and databases it uses, and the quantity of data that requires backing up. It will also depend on a company's policy and regulatory obligations applicable to the organization.

How do I implement a backup policy best practice?

1 Identify your most critical data and plan accordingly

By identifying the most critical data to your business, resources can be allocated to ensure that this data is protected and prioritized. Backups can be tailored to that particular data accordingly.

2 Take frequent backups

If you have mission-critical data, then attention should be paid to the frequency of the backups that are taken.

3 Use the 3-2-1 approach to backups

Create three copies of your data in addition to the original file, using two different backup media types stored locally and one copy stored remotely off-site.

Backups should be isolated or air-gapped from the network when not actively backing up data. Backup media should never be permanently connected physically or over the network.

4 Employ versioning to data

Backups should contain old versions of your data, not just current versions of files backed up most recently. This is important in case of file corruption or ransomware that may be lurking in current data backups.

5 Periodically test the integrity of your backups

Data should be checked regularly to ensure that it is accessible and readable.

Other considerations for your backup policy

- Data should be encrypted when backed up. This will help prevent unauthorized access.
- Consider making your backups immutable, so they cannot be altered by you or cybercriminals.
- Consider using remote storage. Cloud-based storage can be a cost-effective option if managed correctly.
- Automate backups where possible. This will make the practice of backing up your data a part of everyday business.
- Consider the retention period for your backups. This is especially important if you are using cloud services to back up your data. Cloud data storage costs can mount up. So, determine a sensible length of time for storage in your backup policy — and consider legal and regulatory obligations.
- Consider your data retention policy. Do you actually need all the data that you are storing and backing up? Often data is stored unnecessarily adding an unnecessary cost and has additional security burdens if exposed.

Visit us at victorinsurance.ca/cyber.

Further Information

- Government of Canada — Canadian Centre for Cyber Security
  - › Tips for backing up your information
  - › Backup and encrypt data
- Victor cyber resources
  - › Victor Cyber insurance
  - › Guide: "Cyber liability exposures: How to protect yourself and your business from a cyberattack"
  - › Guide: "Cybersecurity: Work securely from home"
  - › Infographic: "Cyberattacks: A threat to all businesses"
  - › Video: "A day in the life of a business owner in a cyberworld"
  - › Video: "Victor experts share preventative measures as cyberattacks on the rise"

#TheThreatIsReal