# Backups

Backups are necessary due to the constant threat of modification or erasure of data due to accidental deletions, malware (including ransomware), natural disasters, or other events. Good backup practices are especially important during critical points of operational cycles, like the beginning of early voting.

Backups play a crucial role in expediting the recovery from malicious cyber activity, allowing the restoration of a system to a reliable state that is free of malware and retains the original data. Rebuilding or re-imaging an infected system from a known good backup or fresh operating system installation is a common best practice in incident response. For instance, if an elections network is compromised due to malware, restoring systems from a clean, uncompromised backup will allow the system to be quickly remediated and put back into production without having to wait to identify remove all possible malicious files.

Backup programs should be developed based on six characteristics:

1. **Data Classification:** Knowing what you want to backup will help you determine what and how frequently that data should be backed up. For instance, data vital to election operations, such as voter registration information, would be considered a high priority, and the risk management process may justify the use of nightly full backups. Retention requirements can play a role in classification.
2. **Frequency:** Consider how much data loss would be acceptable in the event of a catastrophic failure. The amount of data that would be acceptable to lose (e.g., 24 hours' worth) should then be used to determine how often data should be backed up.
3. **Encrypted:** Backups should be encrypted. Having the backup encrypted will safeguard it if an unauthorized individual tries to access it.
4. **Offline:** Backups must be stored offline to reduce the risk of malware infecting the copies. Some malware, such as ransomware, will specifically look for backups that are available on the network to hinder the recovery process.
5. **Offsite:** Backups should be stored offsite to ensure recovery is possible in the event of disasters, such as fire or flooding. Offsite backups could be physical copies or cloud-based. The backup location is vital to the recovery process and must be a place where the backups will be secure but quickly accessible.
6. **Tested:** Testing the backup's integrity and the ability to successfully restore a system from the backup is essential to a successful restoration. This ensures that, if needed, the backups will be able to restore what has been corrupted or destroyed. Too often backups are untested and can't actually be restored in times of crisis.

## Goals

1. Create a procedure for backups
2. Implement automated backups
3. Protect backups
4. Test your recovery plan

## Actions

For Backups, the necessary actions vary by maturity as detailed below.

### Level 1 Maturity

Creating a data inventory for a Level 1 maturity organization should include at a minimum:

1. Create a data inventory to understand the most important data residing within your network. Include, at a minimum:
   - Voter registration information and databases
   - Ballot definitions
   - Election equipment security processes
   - Geopological boundary data and shapefiles
   - Other critical data
2. Ensure data critical to the operation of your state organization or local jurisdiction is backed up and stored offsite.

There are many automated methods for creating backups. Most solutions are encrypted and can be set to the desired frequency. But many are only either offline or offsite, whereas both are necessary to have a complete backup program. Offline backups help protect from ransomware, while offsite backups help protect from local disasters.

Simple built-in backup tools like Apple's Time Machine and Microsoft's Backup and Restore work well for offline backups if they are not kept connected to a network or machine. If you wish to use tools like this, be sure to have a plan to connect them on a prescribed schedule and then promptly remove, isolate, and securely store them. Unless you move them to other locations, they are not good solutions for offsite backups.

Either implement a tool that provides both offline and offsite backup capabilities or implement multiple tools. Some are described below within Cost-Effective Tools.

### Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Ensure that solutions conform to your data management plan.
2. Test backups at least once a quarter and whenever processes or technologies are changed. The goal is ensuring rapidly restoration of operations, if ever needed.

## Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Backup and Recover: A toolbox with links to free tools relevant to this best practice.
- Microsoft® Volume Shadow Copy Service (VSS): Tool to create backup copies or snapshots of files or volumes.
- VeraCrypt: Free, open source, on-the-fly encryption.
- Clonezilla®: Partition, disk imaging, and cloning tool.
- Apple Time Machine: Time Machine is the backup mechanism of macOS, the desktop operating system developed by Apple. The software is designed to work with both local storage devices and network-attached disks and is most commonly used with external disk drives connected using either USB or Thunderbolt.
- Amanda Network Backup: AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup solution that allows the IT administrator to set up a single master backup server to back up multiple hosts over network to tape drives/changers or disks or optical media. Amanda uses native utilities and formats (e.g. dump and/or GNU tar) and can back up a large number of servers and workstations running multiple versions of Linux or Unix. Amanda uses a native Windows client to back up Microsoft Windows desktops and servers.
- Bacula: Bacula is a set of Open Source computer programs that permit you (or the system administrator) to manage backup, recovery, and verification of computer data across a network of computers of different kinds.
- Microsoft Backup & Restore: In Windows 11, you can restore files from a backup created with Backup and Restore or File History.
- No More Ransom: Website to help victims of ransomware retrieve their data, report a crime, and more.

## Learn More

- DHS, CISA, and MS-ISAC Joint Ransomware Guide: A guide written by US federal agencies to assist with ransomware.

## Mapping to CIS Controls and Safeguards

- 11.1: Establish and maintain a data recovery process (Level 1 maturity)
- 11.2: Perform automated backups of in-scope enterprise assets (Level 1 maturity)
- 11.3: Protect recovery data (Level 1 maturity)
- 11.4: Establish and maintain an isolated instance of recovery data (Level 1 maturity)
- 11.5: Test backup recovery (Level 2 maturity)

## Mapping to CIS Handbook Best Practices

- 21, 60

Previous
User Management

Next
Incident Response Planning


Last updated on Oct 03, 2022