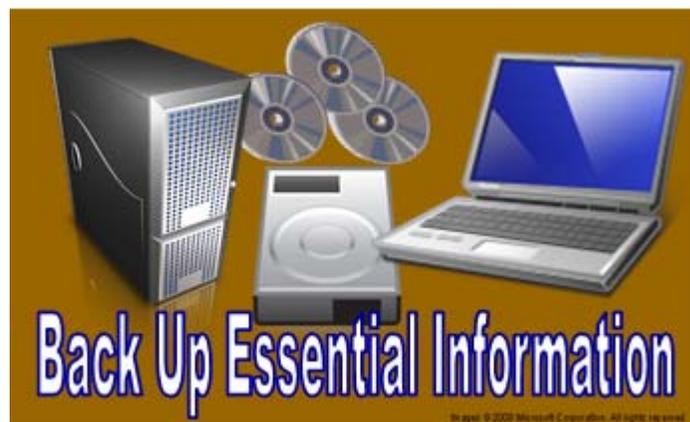


Cyber Security:

Guidelines for Backing Up Information

A Non-Technical Guide

*Essential for
Executives,
Business Managers
Administrative & Operations Managers*



**Multi-State Information
Sharing and Analysis Center**



NYS Office of Cyber Security

This appendix is a supplement to the Cyber Security: Getting Started Guide, a non-technical reference essential for executives, business managers, administrative and operations managers. This appendix is one of many which is being produced in conjunction with the Guide to help those in small organizations to further their knowledge and awareness regarding cyber security. For more information, visit: <http://www.dhSES.ny.gov/ocs/>.

Introduction As an organization's manager you are responsible for the confidentiality, integrity and availability of all documents in your care. Your organization should have formal, routine backup procedures in place to ensure you have access to essential information in the event that your documents, files or even your computer systems are damaged, lost, stolen or otherwise unavailable. The importance of such procedures cannot be overstated, for it is virtually inevitable that at some point in time you will experience an incident that could affect the information in your care: computer system may crash, for example, or your electronic documents could be lost or compromised.

This guide will assist you in developing and implementing a backup procedure in your organization to help protect your information and minimize risks.

What Is a Backup? A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. Backups can be compressed to save space and encrypted to add security.

Think about what information is stored on your systems, e.g. accounting records, email, correspondences, meeting minutes, etc. To avoid prolonged disruptions in your operations, all critical files, as well as any information your organization cannot easily replace, need to be backed up.

Note: Archival storage is different than backup. Archival storage is the permanent maintenance of electronic information valuable to an organization. Archival storage focuses on the storage of digital information that will no longer be changed, but must be maintained uncorrupted and usable for a specified period of time.

Backup Process There are four main components of backup process to provide reasonable protection from loss. Several scenarios are provided below as examples of the importance of a backup process. The remainder of this document explains the backup process.

- 1. Back up data at regular intervals.** What happened: An organization backed up its data once a month, but occasionally less frequently. The organization found the process of backing up tedious and assumed there would be little need to have the most up-to-date data always on hand. Unfortunately, its system crashed in the middle of tax season. The tax collector asked for a backup to the system, and found the last system backup was before tax season, meaning that all information on who had paid their taxes that year had been lost.

2. **Verify the data has been backed up.** What happened: An organization carefully managed its assessment data for properties, constantly updating data and backing up the system to make sure their data would not be lost. To be safe, they produced daily backups of the system and kept each backup for a week until it was replaced by a new one. Subsequently, a computer crash destroyed all their data. When they attempted to restore the data from their last backup, they discovered their backup tape was blank. Although they followed their backup procedures precisely, none of their data transferred onto the backup tapes and all their electronic data had been lost. It took the organization a full month to recreate the data in the system.
3. **Store the backup media in a secure, safe place.** What happened: An organization regularly produced backups of the voluminous records on its system. These included payroll, personnel records, among others. They assumed that the frequency of their backups would protect them from potential record loss. When their main administrative building was flooded, they discovered they were wrong. Although their backup data was stored separately from the computers, they were both stored in the same building, thus they were destroyed simultaneously.
4. **Verify the ability to restore.** What happened: An organization was running two different network operating systems and used the same backup drives and backup software on both. Restores were regularly done back onto the same servers with no problems. When a server running one operating system crashed and its applications were to be moved to a server running the other operating system, it was discovered that the backup software could not restore onto a server with a different operating system. A temporary server with the same operating system had to be set up and the files transferred over the network. That backup software was replaced and cross operating system restores tested.

What to Back Up Understanding potential risks and threats to your organization can guide you in developing effective backup procedures to guard against those risks. The key question is “How much can your organization afford to lose?” To determine the answer, the organization needs to understand its flow of information and the cost of temporarily or permanently losing this information.

In addition to the data used in day-to-day operations (such as financial systems), you should also consider long-term preservation of data that cannot be recreated (e.g., organization’s history or vital statistics records). This may include current files, such as those found on your desktop or server, or other files produced at various locations not linked to a centralized storage area. Software and application files and settings may also need backup to ensure a fast and efficient reinstall of your system.

Backup Media and Devices Choosing the best media type for backups is dependent upon how much data the organization needs to back up and how often. Any type of writeable media can be used as backup as well as any device that can be connected to a computer to copy information. This may

include tapes, CD-Rs, DVD-Rs, external hard drives, or similar devices. Each has its own advantages and disadvantages. The following are common types of backup media:

Tape: Data is stored on magnetic tapes, similar to a cassette tape.

CD and DVD: Data is stored similarly to music CDs or movie DVDs.

External Hard Drives: An external device that uses removable drives similar to those inside your computer. These drives are portable and usually come with backup software.

Flash Drives: A small device that plugs into your computer, also called thumb drives or memory sticks.

Online Backup: Store files on a remote server, uploaded through an Internet connection, eliminating your need to manage tapes, disks or CDs.

Pros and Cons of Media Types		
Type	Pro	Con
Tape	Inexpensive Can be used repeatedly Good for daily backups	Relatively slow Sensitive to heat and magnetism
CD and DVD	Compact Inexpensive Portable	Sensitive to heat Unusable if mishandled Rapidly evolving technology makes today's storage media outdated
External Hard Drive	Most include backup software Can be automated Can be used to replace faulty drives	Expensive Maintaining compatibility with your source systems Sensitive to heat and magnetism
Flash Drives	Easily portable Fast data transfer	Easy to Lose Can be expensive Difficult to label Sensitive to heat and magnetism
Online Backup	Easy data transfer Can be automated	Expensive Provider system can be compromised Provider can go out of business Reliant on provider standards

Backup Process Steps

1. Back Up Data at Regular Intervals

Frequency and types of backups It is important to develop a regular backup routine that reflects the frequency of change in data. If the computer is used daily, it is best practice to back up important files daily. At a minimum, back up all important current files at least once a week. To determine how frequently your organization should back up, think about how much data the organization can afford to lose. If it is a week's worth of data, developing a weekly backup system would be sufficient. If it is a day's worth of data, a daily backup schedule would be necessary. Many organizations collect data electronically, such as tax records, cash receipts, or client documents for example. This information may need to be backed up daily, as it may be impossible to recreate the data, thus the risk of loss is great. In general, it is recommended to replace all backup media every two to five years.

There are three types of backup schedules: **Full, Incremental, and Differential**. An example of these follows at the end of this section. **Full backups** copy every file on the system to a backup device. Many organizations need to schedule full backups during non-operational hours to ensure no files are in use and the full backup can be completed. If possible, full daily backups should be done.

However, incremental or differential backups can be used when there is not enough time to do a full backup. They are frequent backups used to capture new or changed information. An **incremental backup** copies every file that has been created or changed, since the last backup of any type while **differential backup** copies every file that has been created or changed since the last full backup.

The following examples demonstrate the difference between incremental and differential backups. Say an organization does a full backup on Sunday night. Assume that file "A" is modified on Monday, file "B" is created on Tuesday and file "A" is modified again on Wednesday. These files are already on the Sunday full backup in their unmodified versions.

If the organization did **incremental backups**, then Monday's backup would contain "A" in its first modified form. Tuesday's incremental backup would contain just "B." Wednesday's backup would contain only file "A," in its second modified form. On Thursday, when the hard drive fails, the organization would recover the files from Sunday's full backup and the files from each day's incremental backup in the order they were created.

If the organization does a **differential backup** on all other nights, Monday night's differential contains "A" in its first modified form. Tuesday night's differential contains "A" in its first modified form and file "B." Wednesday night's differential contains "A" in its second version and "B." On Thursday the hard drive fails. To recover the organization would first copy the files from Sunday's full backup and then the files from Wednesday's differential backup to have all current versions of the files.

Differential backups can increase in size each day and may approach the size of a full backup. Since each differential backup includes everything in the previous differential backup, many organizations often do not retain all differential backups created between each full backup.

Incremental backups are usually smaller and fairly constant in size from day to day. All incremental backups must be retained until the next full backup is complete. The incremental backup offers the ability to recover any day's activity during the period between full backups. Consequently, if changes were made to a file that should not have been made, the incremental backup can be used to restore the file back to the unchanged form.

To provide timely and flexible recovery, **daily incremental backups** are recommended, with a full weekly backup. It is good practice to devise a series of backups to ensure at least two new backups exist before one is destroyed.

For example: Business A uses a tape backup system. All users save their files to the business' central server. These files are backed up to a single tape, overwriting any data already on it. Backups are done on a daily basis using a series of four tapes. The business also uses a second series of tapes for weekly backups. In this example, the business has determined this is the schedule that best fits its needs based on how much data they could afford to lose:

The Daily group is used Monday through Thursday. The Weekly group is used on Fridays for a full backup.

Day	M	T	W	TH	F
Week 1	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 1
	M	T	W	TH	F
Week 2	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 2
	M	T	W	TH	F
Week 3	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 3
	M	T	W	TH	F
Week 4	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 4

2. Verify the Data Has Been Backed Up

Backup media needs to be reviewed periodically to determine if all of the data has been backed up accurately. Verification can consist of looking at the backup to verify specific pieces of data are there, confirming that files will open, or verifying the total size of the backup is the same size as the original data file.

Backup vs. Archival Storage

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original as a way to ensure business recovery. Backups can be compressed to save space, and encrypted (plaintext or data converted into unintelligible form by means of a reversible translation based on a translation table or algorithm), files contain sensitive and confidential information to add security. Best

practices require that organizations keep multiple versions of backups to increase the chances of retrieving damaged or destroyed information. Best practices also recommend the backed-up file be labeled.

Archival storage is focused on the permanent maintenance of digital information valuable to an organization that must be maintained uncorrupted and usable for a specified amount of time. Archival storage includes one master copy and at least one duplicate copy maintained a safe distance from the master. Unlike backups, stored archival records are the primary copy of the record, not a copy to be used in disaster recovery. Archival best practices dictate that records stored for archival purposes not be compressed or encrypted as such actions might limit the ability of an organization to access and use those records in the future. Information security best practices however, require sensitive or confidential information be encrypted where data is stored.

Sound archival procedures also include media migration, or refreshing, which is the process of copying data from one digital media type to another before the original media becomes obsolete. This process works only if the organization does the refreshing on a regular basis. It must occur before the organization loses the ability to read the data off the media. Digital media have a wide range of life expectancies, but magnetic media, such as computer tape, are generally more reliable than digital media such as CDs and DVDs. Refreshing is most often conducted every five years, but the exact schedule for refreshing will depend on the longevity of the media and whether the media are becoming obsolete. Be aware that no media lasts forever, and factors such as climate conditions and constant reuses can cause the media to go bad.

Electronic data also face the danger of being rendered unusable because the file formats used to store the data are obsolete. It is always best to use file formats that are commonly used and non-proprietary. Open formats, such as TIFF image files or Open Document Format, are formats supported by a number of hardware and software platforms because the code needed to understand the format is published and publicly available. Organizations using proprietary formats, which are formats controlled by a single company, will need to have a plan in place to migrate their data when they change electronic data systems or when the proprietary formats become obsolete.

Additional information on archival storage is available at:

- Digital Preservation Coalition: www.dpconline.org/
- CoOL (Conservation OnLine): <http://palimpsest.stanford.edu/bytopic/electronic-records/electronic-storage-media>

3. Store the Backup Media in a Secure, Safe Place

One of the biggest mistakes made with backups is storing them too close to the original sources, assuming that computer crashes are the only types of incidents an organization may face. To protect its information, an organization should always store backups in a physically secure facility far enough from its office not to be affected by the same fire, flood, or storm that might destroy records in the office. If

backup media remains on-site, it should be stored in a non-adjointing building if possible and in a location secure from intrusion, fire, flood or other natural disaster.

Both backup and archival media should be stored in a physically secure location, ideally an off-site storage facility. Additionally, backups and archives should be protected from access with the same level of protection as working data.

4. Verify the Ability to Restore

It is best practice to frequently test that your backup data can be restored to your systems if loss occurs. Backing up data does little good if it cannot be restored to normal use.

Periodically test that the information can be restored from the backup copies. Periodically review your backup procedures to ensure that all important files are being included.

Provide training so that all personnel understand the need for backup procedures. Ensure that each makes all his or her important files available for inclusion in the backup procedures or follows individual procedures as part of the overall plan.

Summary Your customers and business partners expect you to keep your organization operating at all times. You cannot prevent natural disasters, human error or even malicious acts by employees or others; but you can have a plan that will keep you in business if any of these events occur. This guide has given you some basic information on backup and archival procedures that will enable you to restore your operations when the information you depend on has been destroyed, lost or corrupted. As with all of your important decisions, your approach to backup and archiving should be based on a careful analysis of your organization's functions and the risks to your operations.

For additional information read NIST "Guide to Storage Encryption Technologies for End User Devices" SP 800-111.

The "Cyber Security: Guidelines for Backing Up Information" appendix has been developed and distributed for educational and non-commercial purposes only. Copies and reproductions of this content, in whole or in part, may only be distributed, reproduced or transmitted for educational and non-commercial purposes. (2012)