Back Up Data

What is Backup?

Having a backup these days is mandatory for any organization concerned with their information and data. A file backup is a copy of a file that is stored in a separate location from the original. **Backing up** is making copies of data which may be used to *restore* the original after a data loss event. This new copy of data is the **Backup**. You can have multiple backups of a file if you want to track changes to the file.

Why we Backup?

There are many reasons why your organization may want to back up their data. The primary reason is to recover data after its loss. The loss can occur by accidental deletion, a virus attack, or a software or hardware failure. If any of those things occur and your files are backed up, you can easily restore those files.

Preventing events that result in loss of data is most desired, but backing up data provides the protection for data after a system failure.

Individual computers being backed up are different than servers being backed up. Individual computer users can back up their own information when desired and using methods they desire, whereas data on organization servers need more formal backup procedures.

Backups are ALWAYS necessary. In the event that your computer system fails, it is important to have a good copy of your data saved.

Backup Steps: The Basics

1. Find the files that you want to backup (documents, spreadsheets, databases, etc.)
2. Copy the files to backup media (USB Drive, external drive, cloud storage drive, etc.)
3. Repeat above at scheduled frequency
   Note: this is a rudimentary level of backup. Ideally, you should keep your files organized in folders for easy identification of files needing backup.

Backup Considerations

Method: There are multiple methods of storing backup data. Some methods are described in the Methods of Backups section.

What to Backup: There is a wide range of information that can be backed up. Files that are stored can be backed up on desktops, notebooks, laptops, and servers. In addition, data managed by applications you use such as email programs, client intake programs, homeless shelter programs, QuickBooks, and other programs should also be backed up. An organization should discuss which information is most important. It is important that organization information be backed up whether it resides in the office, and/or on any home computers that people may be working on for office work.

Frequency: Backups must occur regularly in order to prevent data loss. The more scheduled backups that take place the better off your organization. Frequent backups take time, money, and resources but the benefits outweigh these negatives. See Backup Frequency section. Examples of backup frequency are given in the Example of a Backup Schedule section

Storage Location: It is a good practice to keep some backup information offsite. In the event that a natural disaster occurs, your backup will mean nothing if it got destroyed with all the computers and the building.

Security: Whether the backup data is onsite or offsite, you will want to ensure the backup information is secure and accessible only by those authorized to use it to restore lost data. See Security Considerations section.

Retention: The amount of history to be saved is another thing to consider. Depending on the nature of your business, you may want to keep backups that are years, months, weeks, or even just a day old. Keep in mind that the more backups you wish to save, the more space you will need to have (increased cost).

For some data you may be legally obligated to keep 1, 2, 3, or more years of history for your business—it is important to identify what data you maintain carries these legal obligations.

- Ensure that ALL people working with records are aware of any legal obligations.
- Under the Sarbanes-Oxley Act of 2002, most records must be kept for 7 years.
- If you're not sure, check here:
    - http://www.councilofnonprofits.org/document-retention-policies
    - http://www.startnonprofitorganization.com/nonprofits-record-keeping-retention-policy
    - http://siarchives.si.edu/cerp/RECORDS_RETENTION_SCHEDULE_rev2.pdf

Methods of Backups

You can setup regular backups of data in-house (locally), or via an external service (vendor).

Locally-Managed Backups

Many Windows operating systems such as XP and Windows 7 include Backup utilities for setting up regular backups of important files. There are also software packages (free and purchased) that can be used to backup data. In either case, wizards typically guide you through the process of setting up your backup, and include things such as designating the destination device for your backups (see options below), choosing the folders/files to be backed up, and specifying the frequency of backup. Keep in mind that if you use any of the non-cloud-based destination options for your backup data, it is advisable to keep a copy of the backup device contents in a secured location separate from the office.

Backup Destination Options

Flash storage or **USB drives** are forms of storage in which data can be easily erased or edited. The most common form of flash storage is the flash drive. This should be used if your organization needs a cheap, physical, and portable storage. While these may be extremely portable, it is also very easy to lose these drives. It is best to always keep track of the physical location of all external storage devices.

CD/DVD is an easy and inexpensive way to backup up data. CD/DVD storage is known as **disc storage**. This type of storage is digitally recording the data onto the disc. The main problem with this form of storage is size. Often times these discs are limited to megabytes and often times organizational data will exceed that. But disc storage is great for limited amounts of data or data that may have to go to multiple places. The cost of a CD usually goes for only about $.18 cents per disc.

External hard drive allows for the backing up of larger amounts of data than CDs, DVDs, and flash drives. An external hard drive device is physically separated from the computer itself, and is also portable. It operates in a similar way that flash drives do, but allows for the storing of larger amounts of data.

Cloud storage is a service model in which data is stored remotely and made available to users over a network (typically the Internet). It enables you to store your files online with the ability to access and share them from any computer connected to the internet. The files are kept on an external server, and the hosting company makes them available to you online. It offers great convenience, but security and cost are potential concerns.

Many cloud storage options (such as Dropbox, SkyDrive, Google Drive, etc.) work by staying synced with a dedicated folder on your hard drive. Therefore, ensure your backup routine includes that special folder and you will be able to access your cloud storage files in the event of internet outage or other disaster.

Below is a list of some popular cloud storage options. Most services are free up to a certain number of gigabytes. After that, prices vary by the number of gigabytes stored.

Name	Website
Dropbox	www.dropbox.com
Box	www.box.com
Amazon Cloud	www.amazon.com/clouddrive/learnmore
SugarSync	www.sugarsync.com
SkyDrive	http://windows.microsoft.com/en-US/skydrive/download

Vendor-Managed Backups

A backup service is another option where you pay companies that specialize in performing backups for you. Your data is stored on servers they own.

Below is a list of some backup services.

Name	Website
MozyPro	www.mozy.com/pro
Carbonite	www.carbonite.com
Jungle Disk	www.jungledisk.com

Restoring data from a backup service is significantly slower than a local backup since your data is in another location. Also, costs of this service and security of your data must be considered when choosing this option.

Considerations when using a Backup Service

Before storing any files on someone else's server, make sure that the hosting organization is **legitimate**. Do they really host files? Do they have a reputable name? Also it is important to make sure the organization is **trustworthy.** Are the files only available to you? Or are they available to everyone? Last is the organization **reliable**. In the event of a catastrophe, will the backed up files be available to you? Are their servers ever down?

Security Considerations for Backup Data

Security attacks — whether in the form of malicious Internet content, theft of physical devices, login violations, or denials of service (meaning others are prevented from accessing your site) — can catch nonprofits off-guard, especially smaller and mid-sized organizations that may be unaware of possible threats, and unprepared to deal with them once they occur.

Yet data leakage to the public, systems down-time, and reputation loss resulting from such security violations can easily turn away new and existing constituents if such situations are not handled appropriately and quickly. This may, in turn, impact on the organization's reputation and future opportunities for growth.

A computer virus outbreak or a network breach can cost an organization thousands of dollars. In some cases, it may even lead to legal liability and lawsuits. Because of these risks, you should ensure your backup data is protected against unauthorized access.

It is important to **carefully examine any contracts with the off-site backup provider**. This is because another entity will have the actual possession of some of the most valuable assets to your organization. This is why it is mandatory that your organization seek audit rights, and assurance that the company's hiring procedures include thorough background checks. Your organization must to everything in its power to ensure the safety of all assets.

It is also important to make sure that your organization **uses locked containers to transport and valuable assets or information** such as backup data. Locks will discourage some threats and also prevent another customer from inadvertently loading your information onto their own system.

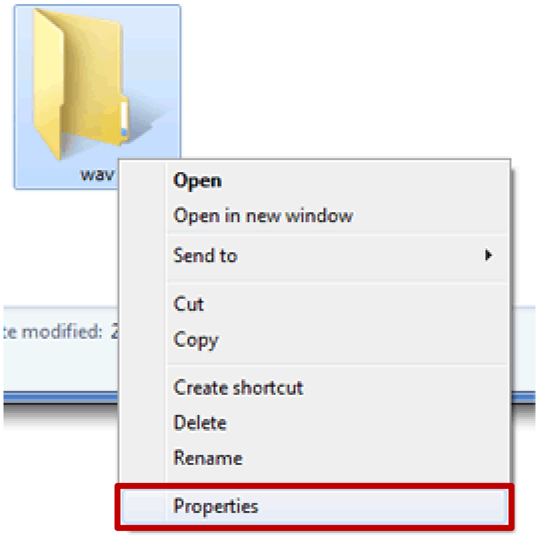
Encryption of data is the process of transforming information to make it unreadable to anyone except those possessing special knowledge. Encryption must take place with any valuable information, including sensitive information in backup data. Not every piece of information should be available to and easily readable by the public. Some data is sensitive and should be protected for safety and privacy reasons.

In order to use encrypted data later on (e.g., if you need to use your encrypted backup data to restore your system after a failure), the data must be decrypted. **Decryption** is the process of restoring encrypted data to a readable format. Some steps for encrypting and decrypting data are below.

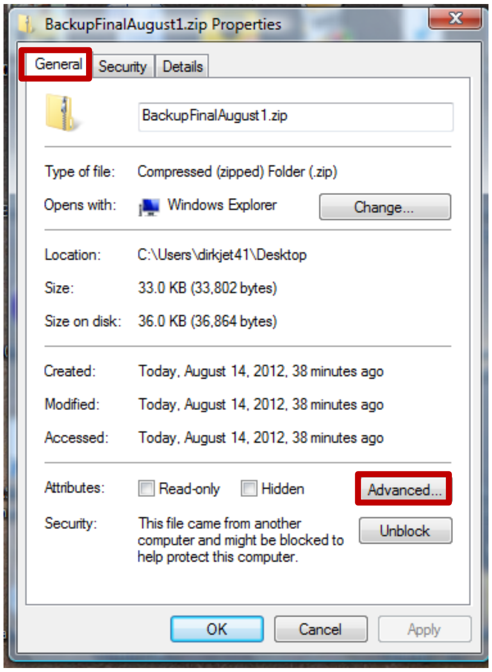
Steps to Encrypt a file or folder

These instructions are for Windows XP, Vista, Windows 7 Professional, Windows 7 Ultimate, or Windows 7 Enterprise.

1. Right-click the folder or file you want to encrypt, and then click **Properties**.



2. Click the **General tab**, and then click **Advanced**.



BackupFinalAugust1.zip

Type of file: Compressed (zipped) Folder (.zip)

Opens with: Windows Explorer

Location: C:\Users\dirkjet41\Desktop

Size: 33.0 KB (33,802 bytes)

Size on disk: 36.0 KB (36,864 bytes)

Created: Today, August 14, 2012, 38 minutes ago

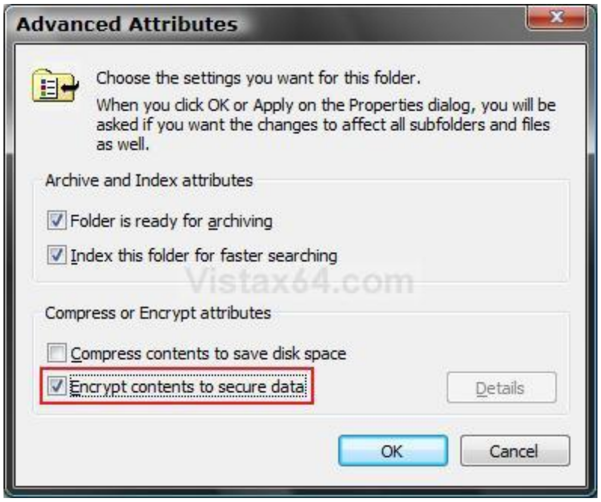
Modified: Today, August 14, 2012, 38 minutes ago

Accessed: Today, August 14, 2012, 38 minutes ago

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

3. Select the **Encrypt contents to secure data** check box, and then click **OK,** and click **OK** again to exit the Properties window.



Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

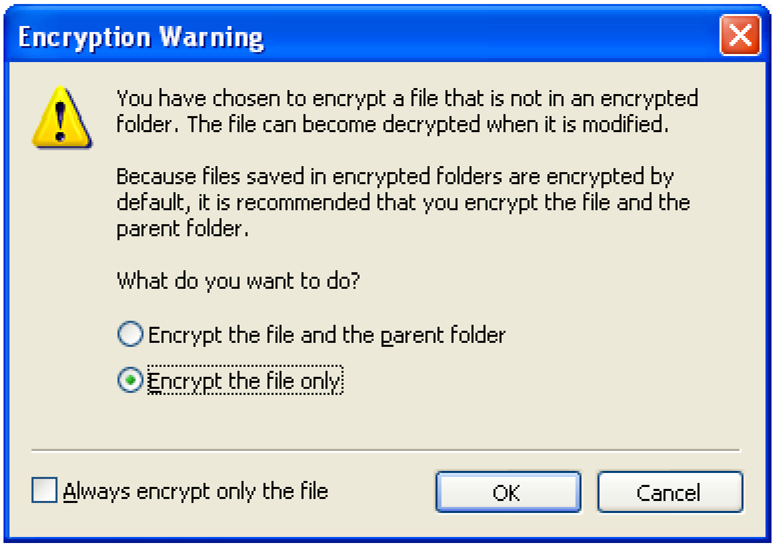
☑ Index this folder for faster searching

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

4. If you are encrypting a file and get an Encryption Warning, click the button to **Encrypt the file only**, then click **OK**.



Encryption Warning

You have chosen to encrypt a file that is not in an encrypted folder. The file can become decrypted when it is modified.

Because files saved in encrypted folders are encrypted by default, it is recommended that you encrypt the file and the parent folder.

What do you want to do?

○ Encrypt the file and the parent folder

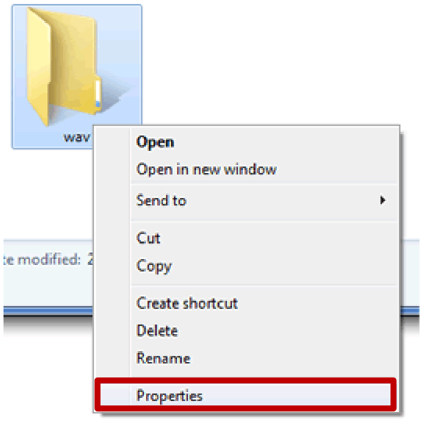
● Encrypt the file only

□ Always encrypt only the file

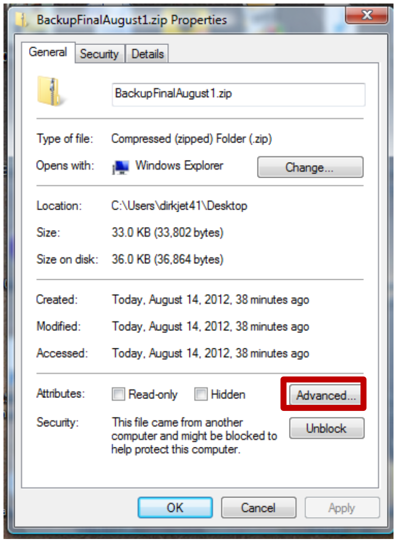
Note: The first time you encrypt a folder or file, you should back up your encryption certificate. The encryption certificate is the “key” that is used if you ever need to decrypt (i.e., use or read) encrypted data again. If your certificate is lost or damaged and you do not have a backup, you won't be able to use the files that you have encrypted. See http://windows.microsoft.com/en-us/windows7/Back-up-Encrypting-File-System-EFS-certificate for instructions.

Steps to decrypt a file or folder

1. Right-click the folder or file you want to decrypt, and then click **Properties**.



2. Click the **General tab**, and then click **Advanced**.



BackupFinalAugust1.zip

Type of file: Compressed (zipped) Folder (.zip)

Opens with: Windows Explorer

Location: C:\Users\dirkjet41\Desktop

Size: 33.0 KB (33,802 bytes)

Size on disk: 36.0 KB (36,864 bytes)

Created: Today, August 14, 2012, 38 minutes ago

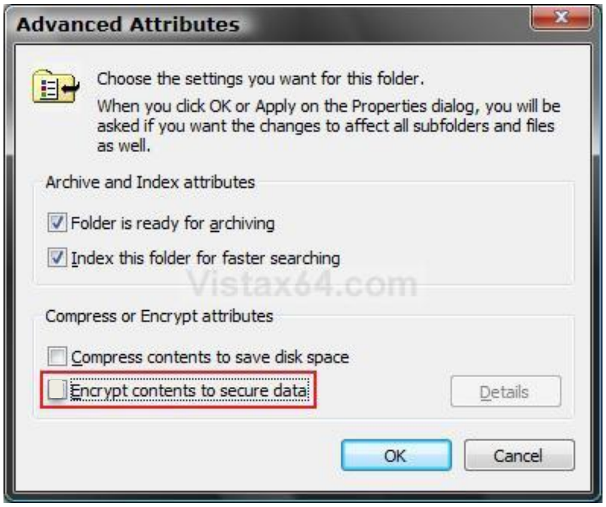
Modified: Today, August 14, 2012, 38 minutes ago

Accessed: Today, August 14, 2012, 38 minutes ago

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

3. **Click the Encrypt contents to secure data check box** to remove the check mark that was previously there, and then click **OK,** and click **OK** again to exit the Properties window.



Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

☑ Index this folder for faster searching

Compress or Encrypt attributes

□ Compress contents to save disk space

□ Encrypt contents to secure data

Backup Frequency

How often you back up your data depends on the number of files or records you create and how often you create them. If you create new files or records every day, you might want to schedule backups weekly or even daily. If you occasionally create many files—for example, if you save a lot of digital photos from a fundraising event, back them up right away and then you may not need to back them up again.

For files that are updated regularly, it's best to schedule regular, automatic backups so you don't even have to think about it. You can choose to have your files backed up daily, weekly, or monthly. You can also back up manually between automatic backups.

Example of a Backup Schedule

The table below is an example of how often you may want to backup organization files depending on how important the information is to your organization, and how often it changes. ***This is only an example***; actual file types, importance and frequency values will vary according to your organization's environment.

Types of Files	Importance of Information[1]	Frequency of Changes[2]	Frequency of Backup[3]
Organization website	Extremely	Quarterly	Quarterly
Email	Extremely	Hourly	Twice per Month
Bookmarks	Not at all	Quarterly	Never
Government forms	Extremely	Quarterly	Quarterly
Financial information	Extremely	Hourly	Daily
HR information	Somewhat	Quarterly	Monthly
Contracts	Somewhat	Monthly	Monthly
Leases	Somewhat	Yearly	Annually
Organization Documents	Extremely	Monthly	Monthly
Templates	Somewhat	Quarterly	Quarterly
Spreadsheets	Somewhat	Weekly	Monthly
Databases	Extremely	Daily	Daily
Contact Information	Extremely	Daily	Daily
Client Information	Extremely	Daily	Daily

[1] Extremely; Somewhat; Not At All

[2] Hourly; Daily; Weekly; Monthly; Quarterly; Yearly; Rarely

[3] Hourly; Daily; Twice per Week; Weekly; Twice per Month; Monthly; Quarterly; Annually; Never