

**External Hard Drives**—There are a number of external hard drives that can be connected to your computer through the Firewire or USB port. Many of these hard drives can be configured to automatically synchronize folders on your desktop with the folders on the external drive. Although this somewhat automates the backup process, these drives can also be easily stolen!

### How to Backup

Backing up your data can be as easy as copying and pasting the files to the backup drive or you can use specialized programs to help create your backup. Most ITS Windows computers have Roxio Easy CD Creator installed. Instructions for using Roxio are located on our website at [smu.edu/help/resources/backup/backup.asp](http://smu.edu/help/resources/backup/backup.asp). For Macs, simply drag the files to the CDRW drive and click Burn. If the built in writable function is not robust enough, you may wish to purchase an application like Toast, to assist in creating your backup.

### Verify your Backup

Once you have created your backup, take a moment to double check that the data was indeed written to the storage media. Simply open the drive to which you backed up the files (CD drive, flash drive, external hard drive, etc.) and verify that the files are there and that you can open one or two of them.

### Protecting your Backup

Once you've created your backup, be sure to label it appropriately so that you can retrieve the data easily if needed. Label the CDs with the date, name and possibly basic information found on that CD (such as email files, work files etc). **THEN SECURE YOUR BACKUPS!** Lock the CDs or storage media in a file cabinet and keep them locked up wherever you store them. Since the files on the backup are not encrypted or password protected, someone simply needs to access the media to retrieve all of your information. If you have a laptop, don't store your backup media in the laptop case. Not only is the information

easily accessible, but if your laptop was stolen you'd be without a machine and without your backup! Treat your backups with extreme care!

Destroy your old backups. As you conduct your backups more frequently, you'll end up with a pile of old backup media. Be sure to dispose of old media properly. CD and DVDs can be destroyed simply by using a pair of scissors and scratching the back of the CD several times. There are also media shredders which work just like a paper shredder leaving your backups in hundred of pieces. Just be sure that the data is no longer readable before you toss the backups in the trash.

Keep a copy of your backup off site. You may wish to store a backup copy at home in the event of theft or a natural disaster. However, backups should be secured even in your home. Remember, files containing sensitive information should remain on campus in a secure location at all times.

## Backup Reminders

- 1. Determine WHEN you will backup your data. Setup a recurring appointment in Outlook or Entourage to create your backup.**
- 2. Determine WHICH files you need to back up.**
- 3. Determine WHICH files have sensitive information and should be excluded from your backup.**
- 4. Determine HOW you will backup your data and purchase media if needed.**
- 5. Determine WHERE you will lock up and store your backup.**
- 6. Implement your plan!**

# Backup your DATA!



A practical guide for  
backing up your data and  
securing your backup  
information

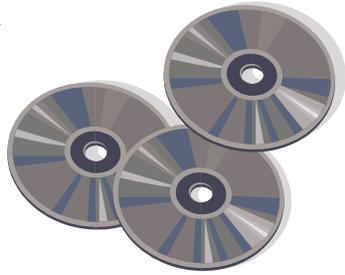
---

This flyer is printed and distributed by the Department of Budgets and Information Technology Services. Additional information may be found at [smu.edu/its](http://smu.edu/its). For assistance, please contact the ITS Help Desk at 214-768-(HELP) 4357

# Backup Basics- A Practical Guide For Protecting Your Information

## Why Backup

Most of us already know the answer to this question. We invest a lot of time, money and resources into gathering and formatting the data files stored on our computers. Without notice, a system failure, virus or even theft could leave us empty handed and scrambling to recreate months or even years of valuable information. So why do we consistently neglect to backup our work on a regular basis? Perhaps it is due to a lack of understanding as to how and what to backup. Hopefully, the following information will help you develop a backup strategy that can easily be implemented.



## What to Backup

It's often a daunting task to determine which files should be backed up. When asked the question, "If your computer was stolen or the hard drive failed, what information would you need most of all?" most users reply, "All of it!" The fact is, personal files such as pictures may be just as valuable to you as important work files. Both should be considered in your backup strategy. Take a moment to identify what types of files you currently store on your computer that you'd hate to lose.

- \_\_\_\_\_ Documents, Spreadsheets, Presentation Files
- \_\_\_\_\_ Email Messages/Folders
- \_\_\_\_\_ Pictures/Music Files
- \_\_\_\_\_ Internet Favorites/Bookmarks

Once you have determined what types of files you wish to backup, determine the location in which you typically save these items on your computer. If you can create new folders and save work files within the My Documents folder, this makes it a lot easier to backup rather than having files saved in locations scattered across your hard drive. In fact, if you always save your files in the

My Documents folder or even on the desktop, you can simply backup your entire profile folder.

The profile folder on a PC is located in C:\Documents and Settings\ProfileName. The profile folder on a MAC is located in Macintosh HD\Users\ProfileName.

**Think twice about files with sensitive information.** Many of the files that we use on a daily basis contain a wealth of sensitive or personal information. For example, many of our work files may contain Student names and ID numbers, financial information, budget codes, etc. This type of information must be guarded with even more care than your work files. If you regularly work with this type of data, you may want to setup a specific folder on your hard drive in which to store this information. When you receive a file containing this information via email, save that file to the dedicated folder on your hard drive and delete it from your email. **The files containing sensitive information, should not be backed up and should not leave University grounds.** Be on the lookout for more information about data encryption if you work with this type of information regularly.

## When to Backup

Determining the frequency of your backup is the next item to tackle. The frequency really depends on your computer usage. A home machine that is used only a few minutes a day, may only need a backup once a month.

A work machine that is heavily used, may require a weekly backup. You may also wish to consider a partial backup (target only critical files) on a weekly basis and a full backup (all files) on a monthly basis. The schedule will vary for each person. The important thing is to set a schedule that works for you and keep it! Consider scheduling a recurring appointment in



Outlook or Entourage to remind you when to conduct your backup.

## Where to Backup

There are a number of backup options available including network drive space, CD-R/W, DVD-R/W, USB drives, external hard drives, etc. It is important to select the right media for the amount of data that you need to backup.

**Network Space:** All SMU employees have a folder on the U drive that is accessible only by that individual. It is not shared and can not be accessed by anyone else. The U drive is a great option for storing several files, but it will not hold all of your data. The U drive may be a good option for partial backups for critical files or a temporary storage space in between complete backup periods.

**CD-R/W**—Most faculty and staff computers are equipped with a CD drive that is capable of writing data to a blank CD. Blank CD-r/w, hold about 700 MB of data. So depending on the amount of data stored on your computer, you may need several disks to capture all of the data. If this is your backup option, be sure to separate the data projects (files included on each CD) in an organized manner. This will help you find and recover the information easily if needed. For example: one CD could store your Email files and favorites, another your work files, and another personal files.

**DVDR/W**—If your computer is equipped with a DVD burner, then you can actually store about 4 GB of data on one DVD. This can make your backup process and storage/retrieval process much easier, as you will only have one media for each backup.

**USB Flash Drives**—These small drives can store a ton of data and make it very easy to transfer files from one computer to another. They can also be stolen or lost easily so be careful using this as your backup media!