BACKING UP AND RESTORING
GENERAL GUIDELINES

1. Overview

All the information you keep in your computer is stored on a hard drive. The important thing to know about hard drives is that they have moving parts − and like all things which move, those parts wear out eventually. So you need to keep a copy of your information on something else as well.

That's not the only reason to keep a copy somewhere else − your computer may be in a fire or a flood. A thief might steal the computer. Lightning might strike it. Or, someone might make a mistake and wipe out your information, without doing any damage to the computer itself. In this day and age, the most common reason for losing data is getting infected and being unable to retrieve your information or even boot up the machine to attempt repair.

So it is to vital store important data somewhere else as well. Not *instead* − most things that you can back your information onto aren't any *safer* than the hard drive. But having your data in two places is safer than one. Having it in three is even safer. Even better is to store your backup(s) somewhere safe. Many companies store backups in a different building or even city − if close by and the building burns down or floods, both the original and the copy could be lost simultaneously.

2. Backup Media

There are many types of media you can back up onto – including removable hard disks, external hard disks, writable CDs, writable DVDs, external flash (thumb) drives, etc. It doesn't matter which type you use – use whatever is easiest for you. If possible, use media with enough storage space to contain all your information on one physical object.

Your backup media (the thing you back up on to) *might* come with software which will ask which files you want to back up, and will copy them onto the backup media for you. You may also use *EVAS Backup and Restore*, which provides an accessible front-end to Windows-based backup.

3. Backup Strategies - Discussion

With as much data as is stored on a modern computer system, how do you decide *what* and *when* to backup? Should you backup the entire system and be done with it? There are several problems with putting your *entire* system in a backup, not the least of which is cost (due to vastly increased storage requirements) and time (how long backups take increases when the entire system is stored).

As long as you have the original CDs for your software, there is no need to include the programs themselves in backups. For example, your operating system and word processor don't normally need to be backed up regularly. Any data files you have created, however, cannot be reinstalled - so you should include them in backups.

Here are some examples of what you might want to backup on a regular basis:

- documents
- email, including important attachments
- anything that you created or would have trouble replacing (including contact lists and extended favorites lists, for example)
- if extensive, collected compressed music (mp3s for example) – actual WAV audio files will take up a LOT of space
- if extensive, collected photos – might take up a LOT of space

- information from any financial software (if you store it on computer)

- anything that would cause *suffering* if it was lost

- anything that would be a *nuisance* if it was lost

- if you have paid for and downloaded software, you should probably backup the install programs (this is one possible exception to the normal non-backing up of software guideline)

You probably DON'T need to backup on a regular basis:

- your operating system, so long as you have the original disks

- your software, so long as you have the original disks

- temporary files (like a web cache, or anything in the trash can)

- anything that you are CERTAIN you won't need if the entire computer becomes rubbish

- anything that is easy or trivial to recreate, re-download, etc.

General Backup Types

1. Full Backup - Everything
Backs up all files, data and programs, regardless of when the last backup was done. This requires the most storage space.

2. Full Backup – Data only
Backs up information files, regardless of when the last back up was done, but restricted to those important items discussed above. Full-featured backup programs allow you to set what will be included – specific folders, files, file types, etc.

3. Incremental Backup – Everything
Backs up *all* files that have *changed* since the last backup was done.

4. Incremental Backup – Data only

Backs up only information (data) files that have *changed* since the last backup was done. Detailed above under 2.

5. Image Backup
This type is different from all the above. This does not actually store *files*, but rather takes a snapshot of the hard drive and retains all the structure and location of everything on the disk. This is the best form of recovery from complete hard drive disaster, as restoring the image will bring back everything – operating system, software, drivers, as well as documents, settings, etc.

Doing an image backup should be limited to:

(a) completely clean and functional machines – you don't want to later restore corrupted or infected operating system files; *and*

(b) important "life" points in the computer. This might include after acquisition and initial setup, or after successful installation of major additional hardware or software.

Backup Plans

How many days worth of information could you afford to lose if your computer crashed? What about if your office or home burned down? What about if most of your city was wiped out by a tornado or a flood? The answers to these questions will tell you how often you should do a backup, and roughly where you should store them.

The "computer crash" one is for your most frequent backup − usually a daily backup, stored in your office or home. The "office−burned−down" scenario is for your next most frequent backup, usually a weekly backup stored in a secure place in another building − possibly a friend's place, or a friendly business whose backups you store.

The final scenario is often a monthly or biennial backup, and is stored somewhere distant − and in some cases, isn't done at all. It's a matter of choice, and what risks you want to take.

Any backup plan is simply a way of controlling risk. You risk losing a day's, a week's, a month's or a year's data − instead of risking losing it all. When devising your backup plan, think about how much risk you are willing to take.

Example Plan - Typical

- After the computer is completely and successfully set up and personalized, do an Image Backup to DVD. Label and store DVD(s) safely.
- Once a month, do a complete full data-only backup (type 2).
- Once a week, do an incremental data backup (type 4).

You can adjust the *timing* of these steps according your work style: maybe you will only need a full backup every six months, and an incremental once a month. Match it to your data needs.

NOTE: Whenever you feel the need (and don’t want to wait for your next scheduled backup), manually back-up particular files of your choice. Example: you are writing the “Great American Novel”, and have just finished a long chapter after five days of grueling effort. After saving the book to your hard drive, it’s easy to manually copy it to a flash drive. Same goes for, say your tax return.

4. Restoring

Restoring is the act of using your previously-stored backups to recover information and put it back on the hard drive.

Make sure you have a method to restore the information from your backup that doesn't involve *using the backup itself*. If your restoration program is only saved as part of your backup, you might not be able to access it to restore your data in a crisis − because to do the restoration you need the software that's in your backup! It becomes a 'catch−22' situation. Usually, having the *installation disks* for your backup program will prevent the 'catch−22'.

NOTE: If your computer will not boot into Windows from the hard drive, and you are using any Windows-based backup, restore should be available if you have the Windows STARTUP disk or through F8 (Repair your Computer).

If possible, under non-crisis conditions, test the restoration process of your backup. If you have a spare computer, test restoring on that; otherwise, test restoration to a separate folder on your main computer − make sure you don't overwrite your primary copy of your information!

(In a perfect world, you would test your restoration process on a computer with a blank hard drive, as if you'd lost your computer entirely and were starting from scratch.)

Guidelines if the hard drive is dead, or you cannot access the operating system:

A) *If you have no image backup:* Insert the operating system disk and boot off of it. Follow on-screen instructions to install the operating system, then drivers from the computer manufacturer. Then install your main programs, and your backup program from

their original disks. Once all the foundation software is reloaded, then restore your information from the backups (step C).

B) *If you have an image backup:* Re-image the system, install any programs (if any) that were installed AFTER the image was taken. Then restore your information from the backups (step C).

If the hard drive is OK, and you are merely restoring data:

C) Restore from the *latest* full data backup you made. Then, *if you are using an incremental back up plan*, follow this by restoring from each *incremental* data backup in order, earliest to last, one by one.

If possible, DO NOT overwrite your current data! [This does not apply to Type 5 – Image Backup – which by definition will overwrite absolutely everything].

System Restore

This is Windows built-in automated backup of *system changes*; However, unlike all the backups listed above, this one IGNORES data. If you have done a Windows update or installed a program or changed drivers or settings and as a result caused problems, you can try to use this tool to jump back in time to before the detrimental change was made, without losing changes you made *later* to your data.

Although Windows tracks changes and attempts to provide useful restore points, it may not have one at the exact time you might need. Also, older restore points are removed to keep the total under a maximum space requirement. If many update/ install/uninstall actions have happened on your machine recently, you might find there is no restore point far enough back to be useful.

If you highlight a particular restore point, a supplied function allows you to view what *probably* will be re-installed or un-

installed if you do the restore. This might help you decide which restore point to use.

If you choose a restore point and confirm it, Windows will reboot your computer and attempt to bring programs and settings back to the date/time you chose. If the restore is successful, check to see if it fixed your problem. If the restore is unsuccessful, you might have to go back into *System Restore* and choose another restore point.