

## ❑ Select an Appropriate Type of Backup

There are a variety of backup systems available to choose from. They include:

- Magnetic Tape (DAT and all other forms)
- DVD+R/RW & DVD RAM
- Zip Drive\*
- CD-RW & CDRW
- Magnetic Optical (MO)\*
- Floppy Disk\*
- Removable High Capacity Hard Drive
- External USB Hard Drive
- External USB Flash Drive

\* Considered obsolete

A professional computer consultant can provide the details on how each system performs. Note that some types of backup may not be suitable for your company. Deciding factors include:

- ◆ Capacity
- ◆ Availability
- ◆ Complexity
- ◆ Redundancy
- ◆ Cost of Ownership
- ◆ Compatibility
- ◆ Failure Rate
- ◆ Support
- ◆ Durability

## ❑ Select a Rotation Schedule or Scheme

The minimum recommended rotation schedule requires eight separate pieces of media.

The first four are used on a daily basis and are used Monday, Tuesday, Wednesday, and Thursday. These are the “daily” backups and are rotated on those days.

The remaining four are used for each Friday of the Month; Friday1, Friday2, Friday3, and Friday4.

This type of rotation provides the option for recovery for each day of the week and for each week of the month. Most errors and missing files will be discovered within this 1 month period.

A more comprehensive rotation schedule would rotate Friday4 (Month1 through Month12) to provide recovery for each month of the year, and would require a total of 19 media. Another possible rotation would include the addition of a quarterly backup. This rotation requires a total of 12 media.

Note that in the example above because the daily backups are used more frequently, they will wear-out sooner than the other media unless they too are rotated or “graduated” within the media stack (know as the **Grandfather-Father-Son rotation scheme**). In other words, at some point shuffle the “Monday” media to “Friday”, then the old “Friday” to “Monthly”, and then the old “Monthly” becomes the new Monday media. This will help to even-out the wear. However, a easier method would be to mark each media as its used, then at the end of a set number of uses replace the media with new ones.

Please note that this rotation schedule is for “complete” backups and not for “differential” backups. Complete backups include all files and not just the changed files (differential) since the last backup. There are several backup rotation strategies, including the ‘Tower of Hanoi’ method. For more information, click this link to see the Wikipedia article on “[Backup Rotation Scheme](#)”

## Automate the backup as much as possible

To be effective, a backup schedule must:

- a) be *easy* to perform
- b) be *convenient* for the operator
- c) be relatively *fast*
- d) include *reporting*
- e) be performed on a *regular* basis

Because people are ultimately responsible for managing the backup process, it should include every one of these points or the possibility exists that the backup may not be completed. Backups may get performed only as an afterthought, and infrequently, providing a false sense of security. Automation is the key. However, it must be implemented carefully. If in doubt, seek the help of professional.

- Easy** → Simple to replace media  
Quick access to the backup system  
Simple to start and stop the process
- Convenient** → Backup time(s) are regular  
Doesn't require extra time or work  
Backup requires only one piece of media
- Fast** → Backup times less than 1 hour if started manually,  
and less than 7 hours if automated.
- Reporting** → Daily printed activity reports or e-mail notifications.  
Specific people designated as backup managers
- Regular** → Performed every day

## Make Someone Responsible for the Backup Process

One common mistake is to assume that someone will take care of the backup. It is important to officially designate a particular person or group of people as backup managers. Make sure every manager is given written policy of what is expected for this position. Include explicit job descriptions and expectations.

## Keep a printed activity log

Most backup software has some form of reporting. If it doesn't, it's time to upgrade to one that provides this feature. After each backup, the manager should print the report, and place it in a "backup" binder. This provides verification that the backup actually worked. Without this report, there is simply no accountability.

## Perform more than one type of backup (Redundancy)

Types include Tape, CD-R, CD-RW, Diskette, MO, Removable Hard Disk, and a variety of other forms.

Reliance on a single type of backup can be problematic, especially during a disaster. For example, if a tape system is used, and the only tape drive available was destroyed, stolen, or malfunctioned, then recovery could take several days while you wait for a replacement drive. If a different type of backup is not possible, then it is recommended that an identical backup system be immediately available. Some companies purchase two

backup systems, one for use, and the other kept in storage as an emergency replacement unit. In the computer industry, products have short cycles. As a result, some backup systems are discontinued as new products are introduced. The problem is *compatibility*. A new backup system may not be able to read the older backup media format. Make sure that the type of backup being used is compatible with current standards, and if not be prepared for problems during recovery.

## ❑ Protect your Media

It is very important to keep your media safe from theft, fire, magnetic fields (magnetic media), or other potential damage. The backup media should have a safe location and a special enclosure. This can be as simple as a media safe (one that is fire rated) located in a locked room.

The goal is to protect the media from:

- ◆ Fire
- ◆ Water
- ◆ Dust
- ◆ Theft
- ◆ Magnetic Fields
- ◆ Damage

If a fire safe is used, make sure it is rated for media. Most fire safes do not provide adequate protection for media, simply because they will melt, even though they may not actually burn.

It may also help to keep a backup off-site at all times. Be careful though, since this potentially exposes your data to espionage. It is recommended to keep your media in a secure location, such as a media bunker or similar type vault. If security is not a concern, then simply allowing your manager to keep a set of backups off-site may be sufficient. **For HIPAA or GLBA compliance, encryption of your backup is required by law.** Again, if in doubt, consult with a professional.

## ❑ Develop a Disaster Recovery Plan

Although not specifically required (except for HIPAA and GLBA compliance), it may be helpful to professionally develop a disaster recovery plan. These documents are written to help your company recover in the event of data loss. These plans are usually very intricate and are individually tailored to each company's needs and thus tend to be costly. However, in the event of a disaster, they are invaluable. One way to determine the need is to perform a cost analysis. For example, if it will cost your company \$100,000 a day in lost revenue and wages to recover from a data loss, then a disaster recovery plan that includes a backup system may be well worth the price. A disaster recovery specialist can help you determine the cost.

When selecting a professional consultant, look for one that is certified in this field. If you want to develop your own plan, look for disaster recovery software and books to help guide you through the process.

**Need more Information? Contact the technical support representatives at Genesys Micro, at (304) 267-0433.**

---

THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. GENESYS MICRO DISCLAIMS ALL WARRANTIES, EITHER EXPRESSED OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL GENESYS MICRO OR ANY OF ITS EMPLOYEES BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF GENESYS MICRO OR ITS EMPLOYEES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.