



HOW IMPORTANT IS YOUR TIME?

Do you verify that your backups have worked?

You would not believe the number of times people assume that their data backup is fine, when in fact it hasn't worked properly. A bad tape or disk, an automatic schedule has not been running when in all innocence you thought it was, or just simple laziness thinking, "I can save some time by ignoring the screen message warning me to take a backup".

And one day when you are relying on yesterdays backup, you get that sinking feeling because you find that it has not been done, is corrupt, or worse still several backups have been missed. You might have to re-enter one days work, a week, or even a MONTH's worth of work. Believe us - a month of re-posting is not funny.

There are many reasons why you might need to restore - hardware, software or network failure, or you do something irreversible in your procedures.

Please - **to save your time**:-

- Verify your backup has worked every day.
- Rotate your backup media and ensure adequate copies.
- Replace bad media immediately you get any suspicious error messages.

Check your data backups before its too late!

NB. The following text can be found in the Millennium Help documentation.

Why should I make backups?

It is very important to make regular backups of your data. Skimping on backups may save time or money in the short term, but this approach is false economy and could be VERY expensive in terms of time and money if your computer goes wrong.

Computers are not perfect and it is inevitable that your computer WILL go wrong eventually. If you have a data backup to restore from you can get working again very quickly once the problem has been resolved.

When should I backup?

You should perform backups on a **daily, weekly, monthly** and **yearly** basis. Each set of media should be stored separately from the others and should be clearly labelled.

How long should I keep the backup media?

You should keep each **daily** backup for at least one week (e.g. 4 disks or tapes, one for each working day Monday-Tuesday).

You should keep the **week** end (Friday) backup for at least two weeks (e.g. 2 disks or tapes to last one month).

Once a **month**, usually at month-end, you should store the backup away for a year. You then have a full 12 months' worth to fall back on (sometimes useful for obtaining information for the auditors).

The **end of year** backup should be kept for a few years at least.

Where should I keep the backup media?

You should keep your backup media clean, dry, away from extreme heat or cold, out of the sunlight and away from magnetic fields. Keep your media in a safe place and as far away from the computer as possible. If the computer catches fire or is stolen you don't want the backups to go with it! The best options are a fireproof safe and/or storage at another site. Make sure the backups are properly labelled as to what they contain, which computer it is and when they were made.

How long can I keep using the same backup media?

You should only use your backup media for a maximum of two years. You should then purchase new media. Replace the media immediately you get any suspicious data verification error or warning messages, and then re-make the backup.

Who is responsible?

YOU are. It is up to you to make sure that the backups are done correctly. If the backup is not working, contact your system support line and get someone to fix it. OPSIS take no responsibility for loss of data due to failure to make proper backups.

Concerning SQL Server Backups

OPsis products use two types of database. The entry-level versions of our software use **Microsoft Access** as the database format, which is a “passive” database (other computers push or pull the data to/from a central computer when needed, by accessing the database directly).

If you are using the **MSDE** (Microsoft SQL Server Desktop Engine), **SQL Server** or **SQL Express** as the database engine for **Millennium Accounts** or **Solicitor Case Manager**, there is a need for you to ensure that the backup is working properly by backing up the SQL Database.

SQL Server is different to the **Microsoft Access** database because it employs an “active” database engine. This engine is “server” software that runs on the central computer listening for requests from other computers (clients), and then “serves up” the requested data (or makes modifications, deletions, and various other performance optimisation and data management functions).

The **SQL Server** database engine runs constantly, and therefore the backup software must interact with the engine in such a way as to take a safe copy of the data, even if other users are accessing or modifying the data. **SQL Server** was specifically designed to ensure backups can be taken while the database is running.

You will need to ensure that you have a version of your backup software that is specifically able to cater for **SQL Server** database backup. This will normally mean that you have to purchase an additional *module* or enable an additional feature. Either way, the backup software must be specifically capable of backing up a **SQL Server** database or it will not be adequate. This is your responsibility.

Additionally, you are advised to take regular “snapshot” backups. Under no circumstances can “snapshot” backups be regarded as a replacement for the overnight comprehensive backup.

There is a facility within Millennium that enables “snapshot” backups to be taken and it will work where the database is a **SQL Server** database. It will backup the database to any internal

How to Backup Your Data

or external drive (note that CD-writers may require. “packet writing” software to work properly, i.e. Adaptec Direct-CD).

There is a facility within **Solicitor Case Manager** (Version 5.1.1 onwards) that will also allow a “snapshot” backup. This will also cater for a SQL Server database and will backup to disk, that can subsequently be backed up to an external drive.

Finally, for those clients with full **SQL Server** or **SQL Express** (not **MSDE**), there is a facility to perform a backup using the SQL Server database management tools (e.g. *Enterprise Manager* or *SQL Server Management Studio*).

Millennium Backup Overview

Millennium has its own built in backup system that enables you to backup your practice databases to protect against computer failure etc. It is recommended that you use this backup system rather than any other, or if you have a main server that automatically backs up overnight, it is still useful to use the Millennium backup to make separate manual backups for special occasions such as software upgrades, month end, year end, and so on.

Backups can be stored on any device that has an operating system drive letter (e.g. A:). Where the data is larger than the media being used it will split the data across multiple volumes. One off backups can also be made to your hard disk.

It is recommended that you use an Iomega Zip or Jaz drive, or a DAT Tape Drive to do your backups. Zip drives are very easy to use and cost effective. Also if you need to send a backup of your data to another party, such as software support, it will be easily readable.

The Millennium backup system will advise you on proper backup media rotation and how long to keep them so you can be sure that you have plenty of good backups to fall back to. e.g. Daily backups, end of week, end of period, end of year etc.

Whilst doing a backup or restore the system locks all users out of the database to ensure that the backup will be successful. When trying to get other users to log out of the database you will be able to see a list of users and machines using the database.

A backup log is kept for each practice database so you can see a record of when your backups or restores were done.

Backup System operation

The backup system can be controlled from the following programs:

Cashier's Desktop

Millennium Practices

The backup system is controlled via the **Backups** menu, offering the following options:

Backup Data - backup one or more practices databases.

Restore from a Backup - restore a practice database from a backup.

View a Backup - view the contents of a backup.



View Log - view the backup log.

Remove Database Lock - (Millennium Practices program only) removes a database lock. If you crash out when making or restoring a backup a backup lock file will be left, preventing you from logging in. This will allow you to remove the lock file.

Setup - setup the backup options.

Backup media required and storage times

The backup system keeps the following regular backups:

Daily backups - are made each day and must be kept for at least 1 week.

Daily Monday

Daily Tuesday

Daily Wednesday

Daily Thursday

Week-end backups - are made at the end of the week (usually Friday) and must be kept for at least 2 weeks.

Week end 1

Week end 2

Period end - are made before moving to a new period and must be kept for at least 2 periods.

Year end - are made before moving to a new year and must be kept for at least 2 years.

To store the above backups you will need at least 10 backup sets. Each backup set will consist of one or more volumes depending on the size of your databases and the media used.

When making backups Millennium will advise you how to label your backup sets, how long to keep them and when you can overwrite them.

File types used

The backup system uses the following file names during various operations. The practice database path and filename is used with a different extension.

dbname.blg - is the backup log file. All backup operations are logged into this file.

dbname.blk - is the backup lock file. When this file exists no one can log into the database.

dbname.rst - is a temporary restore file. When restoring a practice database and overwriting the current one, it first restores to this work file. When the restore is successful the database will be overwritten.

The backup data wizard allows you to make a backup of one or all of your practice databases.

Access this window from the **Backups** menu in programs that support the backup system.

Use the **Next** > button to move to the next screen and the < **Back** button to return to the previous screen. If you want to cancel the procedure, use the **Cancel** button.

The following sections describe screens that you may see as part of the backup process.

Select practice database to backup

Choose what practice database to backup.

Backup this practice only - just backs up the practice database shown.

Backup ALL practices - backs up all of your practice databases in one go.

Backup destination

Choose where the backup will be written to:

Usual drive for a regular backup - will do your normal backup to the usual drive. You should use this option most of the time because you can only do a regular backup with this. Set the option for this default drive in the backup Setup.

Other removable drive - allows you to select another drive that takes removable media.

Different location ... - you will be asked to enter a file name to create a backup archive in any directory that you wish.

To verify that the backup has been written correctly, tick the **Verify backup** box. If you do verify the backup it may take twice as long to do.

Backup type

Choose the backup type:

Regular backup to usual drive - makes a regular backup in one of the following categories. The correct category to use will normally be selected for you. e.g. If you answer yes to making a backup in the period maintenance program it will select period or year end for you.

Daily

Week end

Period end

Year end

Separate one off backup - use this to make a special backup that you can call what you like. You must enter a Backup description.

Current database users

You will see this screen if any of the databases you want to backup have people using them.

A list of users that have the practice database open will be shown. Each user is identified by their Windows machine name (not the Millennium login or machine name).

If a user is in Millennium and tries to do something they will automatically be logged out. If a user has a database open in some other way (e.g. from a spreadsheet) you will have to tell them to log out.

Wait for the users to log out and then use the **Retry >** button to try again. Repeat this procedure until all of the users have logged out.

Backup is ready to start

The practice(s) to backup are shown with the name of the backup archive to create.

If you are doing a regular backup you may be told if you can overwrite an existing backup.



OPSIS™
SOFTWARE & SERVICES PART OF IRIS

How to Backup Your Data

Backup progress

This screen lists the files that are being put into the backup archive and shows you the progress.

Labelling and storage

The backup has now been successful.

You will be told what label to put on your backup media.

If you have done a regular backup you will be told the minimum time you should keep the backup.

Use the **Finish** button to close the window.