Why backup is so important!

Catastrophic failure of your data is a real possibility.

- Your data access can be blocked by Ransomeware
- Natural disasters can destroy your network. (Fire, flood, hurricane, etc)
- A server component could fail such as the server hard drive.
- A virus or malicious employee could destroy your data.
- Computers along with backup media could be stolen.

Windward Software on-premise products do not have an automatic backup function. Your backup in your business should include more than just Windward Software data such as your PCI Encryption Key, spread sheets, documents and other files that support your business processes. We recommend you have your network technician configure and test your backup & archive process.

Without a backup, you can seriously impair your ability to run your business and Windward Software may not be able to re-create your lost information. **Your backup is only as good as your ability to restore.**

If you are hosting in our System Five on Cloud environment the following is our backup schedule. Windward Software does not offer backup services to on-premise installations and are not responsible for your on premise system backup.

Getting everyone out

- **WARNING: if anyone is logged into your data, the backup/copy will not be fully intact/corrupted.** (Ex: logged in means has any System Five Screen Open, connected to polling etc.)

To have a clean successful backup everyone should be signed out. To ensure this there are two methods available.

1. Have your backup program create a file GETOUT!.NOW in the data folder. Any users still signed in will receive a three-minute warning before the system will shut them down. Note, make sure that after your backup is complete, the GETOUT!.NOW file is deleted. If it is not, then you will be unable to login to System Five.
2. In the Setup Wizard, Enable the “Time Out Settings” to have a time period when users can not sign in.
3. Alternatively, to confirm that everyone is out of the Live environment run File Check (Setup Tools –> Utilities –> File Check). Click the “Continue, I have done a backup” button. The next screen displays a “List of Users Signed in” to the current environment. If there are no users signed in to the environment, this screen should not list any users. Click Quit to exit. ***Note:** This method will not prevent users from logging in after confirming everyone is out via the file check or subsequently anytime during the Backup procedure.

For information on preforming a manual backup click here.

WARNING: Export PCI Encryption keys or backup will be useless

The PCI Encryption keys need to be backed up as well. These can be exported to a file and backed up. Most customers have some encrypted database files. The key to opening these encrypted files is in the registry of your PC's. A normal backup to a memory stick does not include this information. You must periodically export your PCI Encryption keys, so that if your offsite backup is all that is left, you can still have access to any encrypted pervasive files. This could be critical files only, all files, or somewhere in between.

- The PCI Encryption keys are like the combination to a safe. Your encrypted data is like data in a safe. If you take the safe home and leave the key on top of the safe, you are not really protecting the data in the safe all that well. Please consider this carefully, and DON'T store them with the backup.
- Whenever you rotate the PCI keys, make sure to export them. You can store them on a separate external drive, another USB key, or other. Again, DON'T store them with the backup.

How to Export the PCI Keys

1. Open the “Setup Wizard” and scroll down in the left-hand window and click on “Payment Processing”.
2. In the right-hand window, in the “Credit Card Info” tab, click on the blue Hyperlink that says “PCI Compliance Check”.
3. This will open another popup that says “PCI Check - Payment Card Industry Security Program”.
4. Click on the “Key Management” button which will open the “Exchanging Encryption Keys” window.
5. Click on File and Export. Save the file to a convenient location such as your desktop, or the System Five Folder, so that it can be copied to a safe place such as a USB stick.

Best practice is to store these keys separately from your normal data backups. The reason being if someone gains access to your backup, they would have the ability to restore it to their own computer and decrypt your data.

On Premise Backup

- Work with your local IT professional on the design and operation of your system/network backups. Windward Software does not offer backup services and not responsible for your on-premise system backup.
- What to back up is important
  - Backup the data directory and all folders contained within it (Use help > about menu, the shared directory is the directory you want).
  - Store a copy of the current executable files from the bin directory (use the help > about menu looking at the directories section for more info)
  - Save a copy of your PCI Encryption keys (All data sets have encrypted files)
- Good ideas:

    - Make at least 1 week of daily backups so they are available at any time
    - Archive each month-end backup
    - Backups should be stored off-site in the event of fire/flood etc.
- CRITICAL ISSUE: test your backups by restoring them to training.
    - Also, it is important to try to restore your data to a fresh machine (ex: a laptop that has never had System Five installed on it). To prove that you can do the restore if you lose everything.

Best practices in backup

Consider these best practices for configuration and backup regime for your on-premise server and data.

1. Use Shadow Copy (also known as Volume Snapshot Service, Volume Shadow Copy Service or VSS) is a technology included in Microsoft Windows
2. Have your users signed out and even consider stopping the Pervasive services to ensure the Pervasive database has cleanly flushed any cached data.
3. Backup often as you don't want to have to retype your information. (For most businesses this is daily.)
4. Have several backup media, not just a single source. (For most businesses this is USB or external drives.)
5. One backup media for each day of the week your business is open, four week ends, two month ends and a yearly.
6. Take the backup's off-site. (Most business owners or the person in charge of backup takes the last backup home with them.)
7. Verify your backup to see if you would be able to restore from it if it became necessary. (Most businesses do this yearly.)
8. Archive a backup from each month end so you can refer back to them in the future. Particularly valuable for inventory value detail.

What tools can you use?

1. Microsoft operating systems since Windows 2000 have come with a simple backup solution. This can be found from the Start menu, Programs, Accessories, Systems Tools and choose backup.
2. Offsite backup solutions are an option, the disadvantage with these is restore time is based on your internet speed which may be an issue to consider if you have large amounts of data.
3. Actian does have a Pervasive Backup Agent which can be used.
4. Any other backup solution that allows you to backup and restore your information.

A snapshot while the database is running and users are sign in using System Five can leave your database with integrity errors or even corruption. We do not recommend using snapshots as a method of backing up your data.

What to backup for System Five?

1. Windward System Five data is normally stored in \System5\data folder. This is all your business information so back this up.
2. Windward System Five application is normally stored in \System5\bin folder. This program folder is needed to run with your data. If you choose to not backup this folder, you can choose to download the latest released version of our software if you were restoring but a data conversion may be required if you were running an older version.
3. Export your PCI keys

To check where your data folder is located

1. Sign into your Windward Software version.
2. From the help menu, choose about.
3. Find the “Data Directory” and this is the location of your data.

Clearing the No Backup Detected Warning Message in System Five

There is a file in your “data” folder called backup.dat (for older version of System Five, it is called backup.btr) which is attribed daily with an archive bit. If this archive bit is not cleared after your backup process is performed, the “No Backup Detected” warning message is displayed in System Five when logging in for the first time. Most enterprise level backup softwares have the facility to clear such things as an archive bit on a file, or have the ability to run a program after a successful backup.

- If that is the case, then have your backup software clear the archive bit on the Backup.dat file OR
- Execute a simple batch file that executes the command: **ATTRIB BACKUP.DAT -A** This will prevent the No Backup Detected warning message from displaying after a backup has been performed.
- You can also clear the archive bit with Windows explorer after each backup. Find your backup.dat file in your data folder and right click and choose options. Click on the “Advanced” button and uncheck the option “File is ready for archiving”. And then have the file READ ONLY.

From:
https://wiki.windwardsoftware.com/ - **Windward Software Wiki**

Permanent link:
https://wiki.windwardsoftware.com/doku.php?id=faq:backup

Last update: **2020/09/18 10:11 (4 years ago)**