SECMON1

Information Security Guideline

Backing Up

THIS PAGE INTENTIONALLY LEFT BLANK

The concept behind backups is simple: Make a copy of your files and configurations and place them on storage separate from your main hard drive. That storage can be another drive, an external drive, a NAS, a rewritable disc, or an online storage and syncing service. Should you lose the files, either through disaster or by permanently deleting them, you can just restore them from saved copies.

In order for this to work, the copies must be updated regularly. Most backup software allows you to schedule scans of your hard drive for new and changed files daily and some even continually (or at least every 15 minutes) monitor your drive for changed or new files.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about daily backups and why it is an essential security measure.

In this document, we are going to describe how to implement some basic backup strategies as well as take you step by step through some ways you can achieve this using your existing technology and resources. Finally, we will give you some interesting and important links where you can educate yourself further on the topic and discuss some other options available to you.

Software Applications

There are some vendor-provided backup solutions available. Below are a few of them and of course there are others.

- Acronis
- StorageCraft
- Paragon
- IDrive
- BackBlaze
- Carbonite
- Crashplan
- SOS Online Backup
- EMC MozyHome

Implementation Guidance

Data is your most important digital asset. Protect it with daily back-ups. Similarly, back up your software and configuration settings every time they change. Store back-ups offsite, if possible, and retain for three months. Test as appropriate. Backups will contain undamaged copies of files. Store backups offline or otherwise disconnected from computers and the network. Implement a backup strategy that minimises (or even eliminates) dependencies so that a version of files can be restored even if other versions have been encrypted, corrupted or deleted. Finally, ensure your organisation's incident response process identifies and restores all files that have been maliciously modified or deleted.

Note: Encourage users to avoid storing data on local storage media such as their computer's hard disk or USB storage, which is unlikely to be backed up. Instead, use corporate file servers and ASD certified cloud services.

Granular options for backups include whether they are full, incremental, or differential.

- **Full**: All the data you've selected for backup is copied in its entirety
- **Incremental:** Saves system resources by only backing up changes from the last incremental backup. You need the latest full backup and all the intermediary backup data to restore a file to its original state.
- **Differential**: Saves all changes from the last full backup. You only need the last set of differential backup data and the first full one to restore a file to its original state.

Password protection and encryption are usually available options when setting up your backup. Using both is a good idea if the data you are backing up is at all sensitive.

Another option offered by many backup applications is versioning. This allows you to specify how many previous versions of your files you want to preserve, and for how long.

A step further is copying the entire hard drive, including system files, this is known as a *disk image*. This contains every bit of data on the drive and offers stronger protection, since it enables you to recreate a system after a hard drive failure. Some products can even update a disk image nearly continuously. However, that extra protection comes at the price of being more complex to set up and to restore.

Another recommended approach is online backup (or cloud backup). Services like IDrive and SOS Online Backup securely send your data over the Internet and save it on remote file servers in encrypted form. The big plus of this option is that the data is off your premises, and thus not susceptible to local disasters. The downside is that they tie you to annual fees, and uploading and downloading backups is slower than loading local copies. Some online backup services, such as CrashPlan and SOS Online Backup, include software for making local backups.

Further information

Further guidance, including applicability for non-Windows operating systems, is available at ASD Strategies to Mitigate Cyber Security Incidents.

Backup Strategy

What to Back Up

While it seems obvious to point your backup software to your documents, pictures, videos, music, etc, there are other items that are important to backup.

E-mail

It is unlikely that your e-mail software (if you use that instead of Web-based e-mail such as Gmail or Outlook.com) will place your e-mail data files in an obvious place for backup. It will be up to you to make sure you know where they are located.

Users of Microsoft Outlook (the desktop version) have to keep track of a file called the PST (Personal Storage Table), which holds all of the e-mail you've downloaded (eg, name.pst). It could be located in a couple of places, depending on which version of Outlook and Windows you are running. To find it, open Outlook, go to File > Account Settings > Data Files tab, click any entry, and Open Folder Location. You also need to make sure you can See Hidden Items – in File Explorer, there is an option in the View menu to show hidden items.

You can back up the PST manually, but it can get really big. Outlook has an Import and Export option that helps. Instructions on exporting Outlook files to pst can be found here. It is recommended, though, that Outlook is used only with a service that stores the email on the server like Outlook.com, Gmail, or a work account through an Exchange Server or IMAP. Then the e-mail is out in the cloud, but also in an OST (Offline Outlook Data File) format, which can be backed up separately.

Drivers

If you have hardware peripherals attached to your computer, you've got drivers. Drivers are the software that allow your PC to talk to video cards, printers, scanners, etc.

If you neglect backing these up, you may have to search every manufacturer's website to get them when performing a restore.

Configurations

It's a good idea to backup your system configurations so as not to lose system stability as well as security settings.

Everything

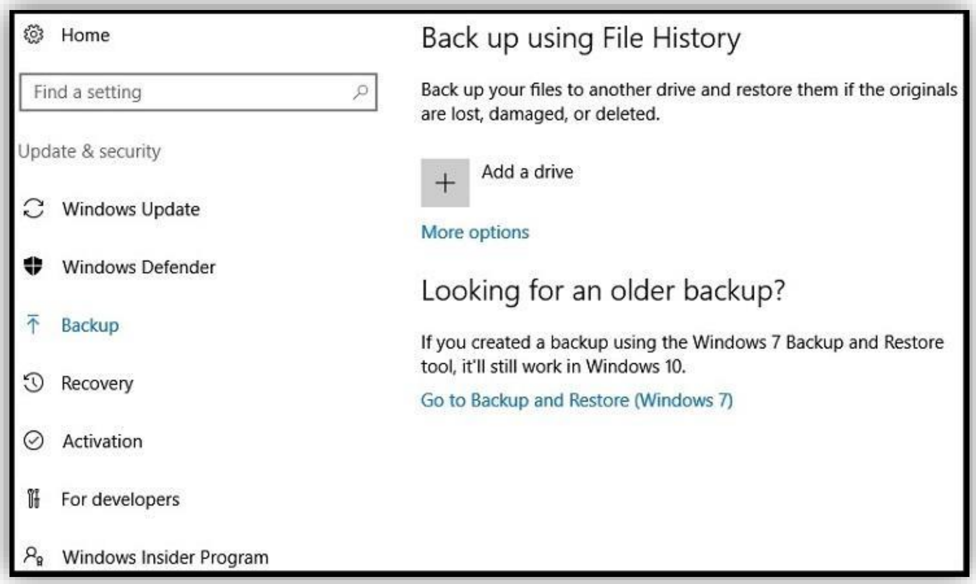
As mentioned earlier, it is necessary to have at least one full backup to revert to. You can elect to do daily backups of changes that have occurred (as well as keep different versions, just in case) as well as new files that have been created.

Types of Backup

Select Files and Folders

If you only need to back up specific data, use software that will let you pick which files to save. **Note**: Simply moving a file isn't backing up. You need at least two copies). Back up entire folders to ensure newly created or updated files get backed up at a later date. Also label your backups with time and date.

Windows has an integrated Backup and Restore feature available since Windows 7. It can be found in the Control Panel. It lets you create a full system image or even create a repair disc for when Windows crashes or breaks. A system image is a full copy of your entire Windows system drive as it exists – so if you ever have to restore it, it will be exactly as it was on the day of backup.



Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Looking for an older backup?

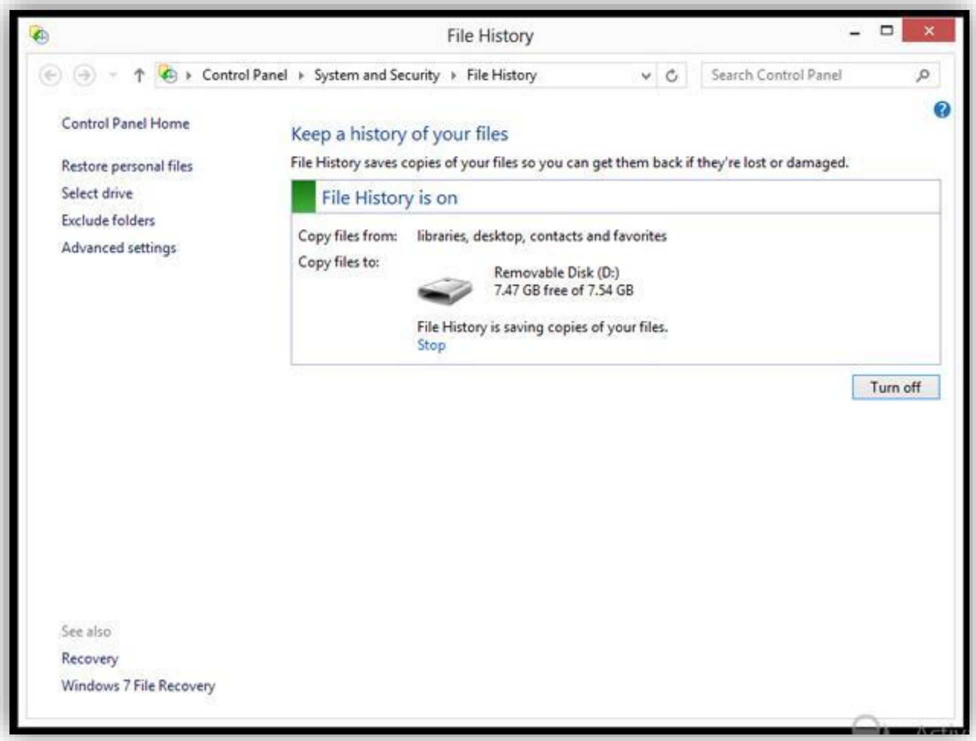
If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

There is also a **File History** backup option. Like Backup and Restore, it offers recurring copying of files you use to a secondary drive as backup. You click the **+** icon when your secondary drive is available and it will try to locate it automatically. File History is a lot easier to set up, but also more limited.

How to Set up a File History Backup in Windows 8 and 10

1. Type **File History** from the start screen or in the search box, and select **Settings.** Click on **File History**. From here, you can choose a storage location for your automated backups.

As with any backup, it is a good idea to use an external or network drive instead of your local disk, in case the system becomes unresponsive or compromised.



Keep a history of your files

File History saves copies of your files so you can get them back if they're lost or damaged.

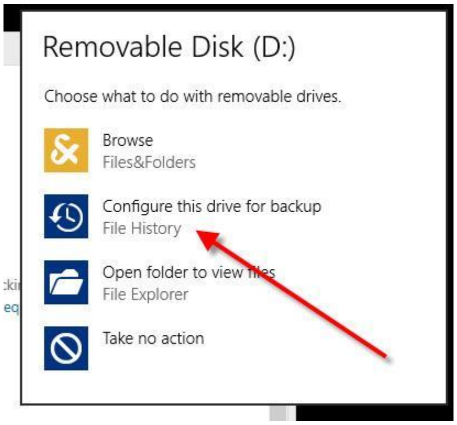
File History is on

Copy files from: libraries, desktop, contacts and favorites

Copy files to: Removable Disk (D:) 7.47 GB free of 7.54 GB

File History is saving copies of your files.

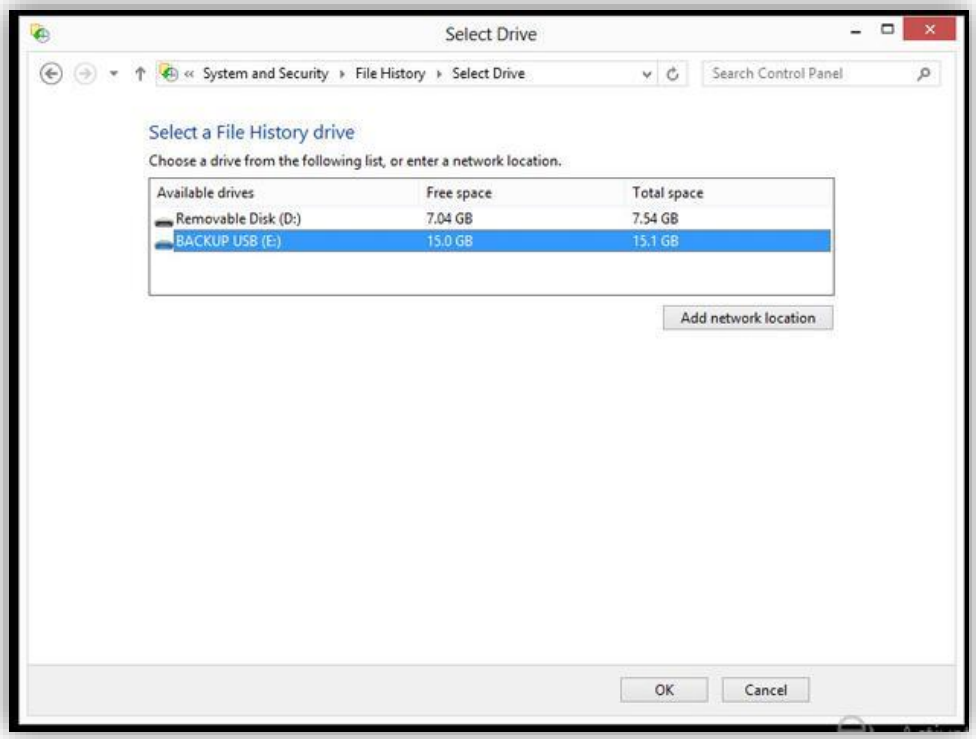
Note: When you first plug an external drive, a notification panel will pop up asking you how you want to use it. Choose **Configure this drive for backup – File History**.



Removable Disk (D:)

Choose what to do with removable drives.

2. This will open File History's **Select Drive** dialog, and all you have to do is select **OK**. The main File History dialog will then display, with a green mark followed by the text **File History is on**. You can turn it off with a button at the bottom of the dialog.

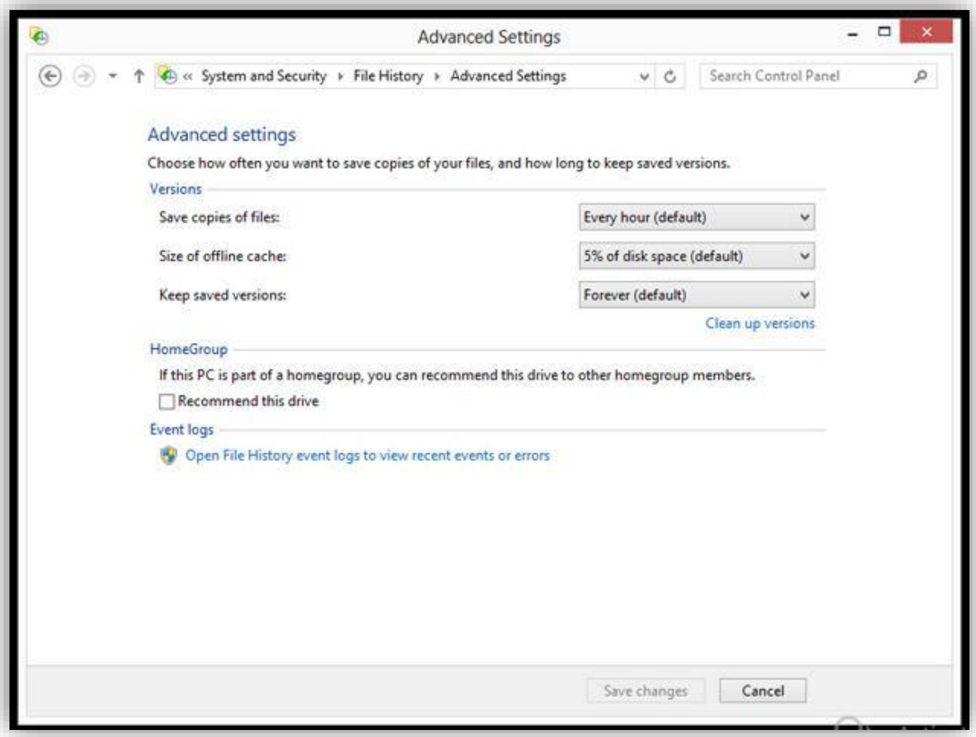


Select a File History drive

Choose a drive from the following list, or enter a network location.

Available drives	Free space	Total space
Removable Disk (D:)	7.04 GB	7.54 GB
BACKUP USB (E:)	15.0 GB	15.1 GB

3. You have some options for how this feature will work. You can change the backup drive and exclude folders from being backed up. By default, File History saves snapshots of all files in your Libraries, Contacts, Favorites, SkyDrive, and the Desktop. This makes sense, but you may have subfolders you don't want included. Unfortunately, you can't add just any folder – it has to be under one of those main folders. You can always add any folder to a Library, which is a way around the problem.
4. You can fine tune things even more by choosing Advanced Settings. Here you can choose how often to backup files: The default is once an hour, but you can set from every 10 minutes to daily. You can also set how much disk space to devote to the backup – from 2-20%.



Advanced settings

Choose how often you want to save copies of your files, and how long to keep saved versions.

Versions

Save copies of files: Every hour (default)

Size of offline cache: 5% of disk space (default)

Keep saved versions: Forever (default)

Clean up versions

HomeGroup

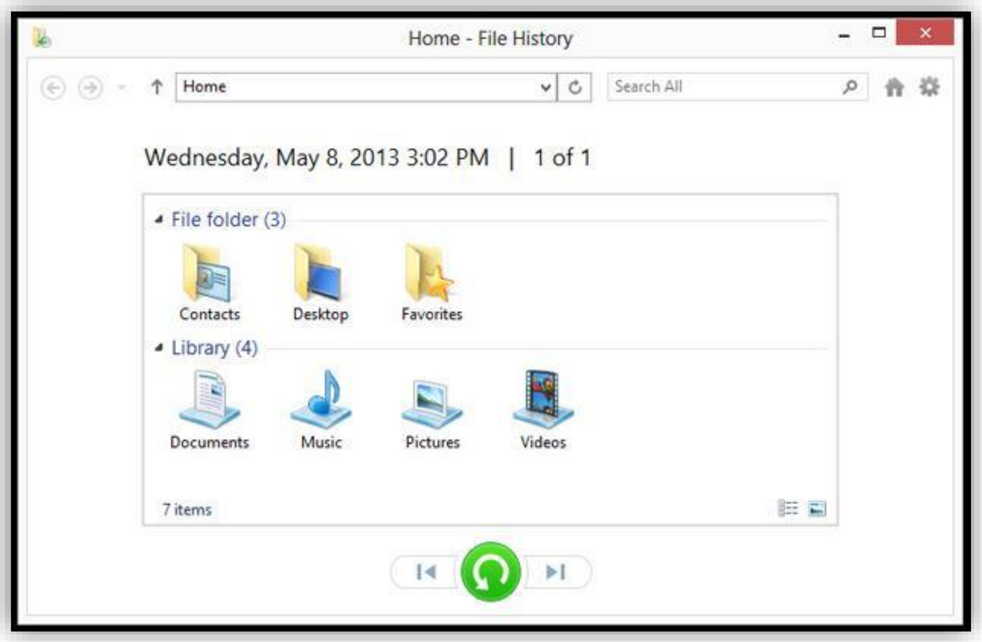
If this PC is part of a homegroup, you can recommend this drive to other homegroup members.

□ Recommend this drive

Event logs

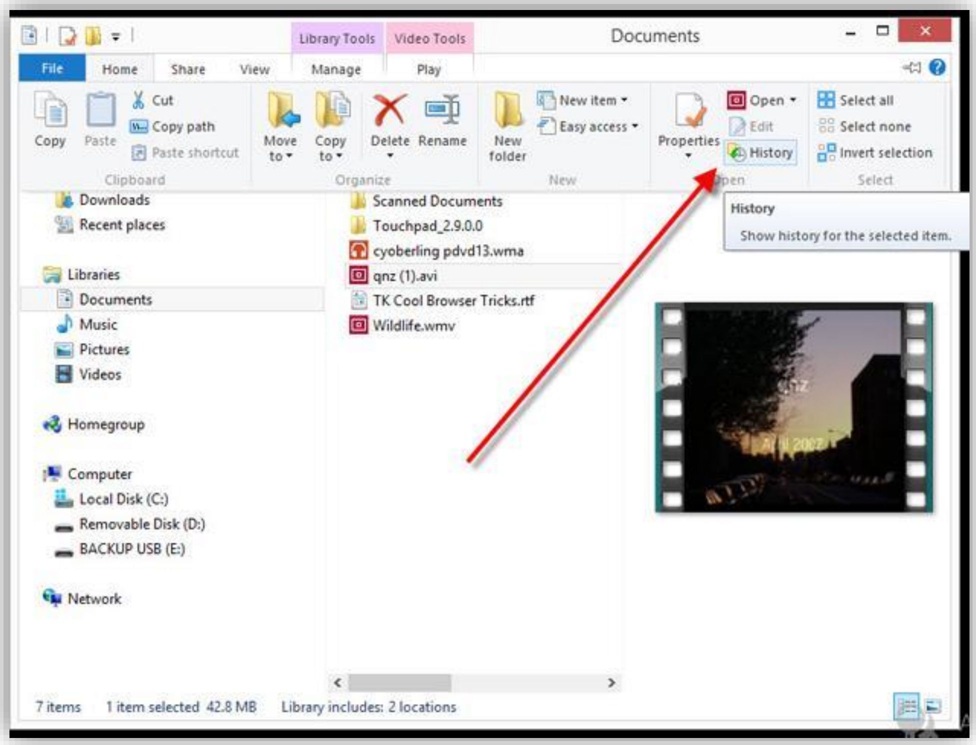
Open File History event logs to view recent events or errors

5. Another helpful option is the ability to set how long you want the system to retain the backed up files. The default is **Forever**, but you can make the backups go away after 1 month, 3 months, 6 months, 9 months, 1 year, or 2 years.
6. To restore, just open the **File History** dialog (type **File History** at Start screen or in search box) and choose **Restore personal files**. This will display all the covered folders. You can restore whole folders or individual files if you drill down into the folders. The big green circular arrow will restore them to their original location, but you can also choose **Restore to** from a right-click (using the mouse button on the right) menu or from the Settings gear to specify a target folder.



Wednesday, May 8, 2013 3:02 PM | 1 of 1

7. Next to the green circular arrow are back and forward buttons, which let you choose the previous or next saved versions. If you click the back button, even deleted files will show up, available for restoration.
8. You can also get to the File History dialog for restoring previous versions through Windows Explorer. With its ribbon set to Home, click on the History button, at the bottom of the second-to-last column on the right. If you do this with a file selected, you'll be able to revert to versions of just that file; otherwise you'll be able to retrieve the earlier versions of all files in the folder at once.



Cloud Storage and File Synchronization Services

This option is good for anyone with more than one computer in use. Synchronization software ensures you have the same files on all your PCs. They always include a backup of files online, which you can access anywhere, even via smartphone. Big names in this area include Dropbox, Microsoft OneDrive, and Google Drive.

With any of these, make a change to a file and it's automatically sent to all the other PCs using the account, even on other operating systems.

Online Backup Services

Online backup services are becoming the norm for backing up important files. Unlike the above services, which include a file-sync option, straight backup products lean toward direct transfer of files from a hard drive to online/cloud storage, with easy restoration options.

You install software on the PC, specify what files/folders to keep backed up, and it does the rest in the background. Because the storage is online, you can typically read files via the browser, or restore the files to other systems, as needed. Big names are mentioned above: iDrive, CrashPlan, Carbonite, and EMC MozyHome.

Full Disk Image

There are many ways to back up an entire hard drive. The first: copy all the files from the drive to another larger drive. This means you get everything, even if you don't need it, but it is easy to keep up-to-date and restore select files from it as needed.

Another method is to make an image of the drive. An image is a replica of all of your data, even the programs and system files, taken like a snapshot in time of the drive at the given moment. When used for restoration, it overwrites what exists after that point in time; the hard drive reverts to the exact state it was in at the time of backup.

Note: Imaging will not include data accumulated after the original imaging. Data should be backed up separately.

Final Note

SECMON1 are available to review your backup strategy and configurations with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement a backup solution for your company.

Please feel free to visit our website at www.secmon1.com

You can also reach us by phone at 1300 410 900 or by e-mail at contact@secmon1.com