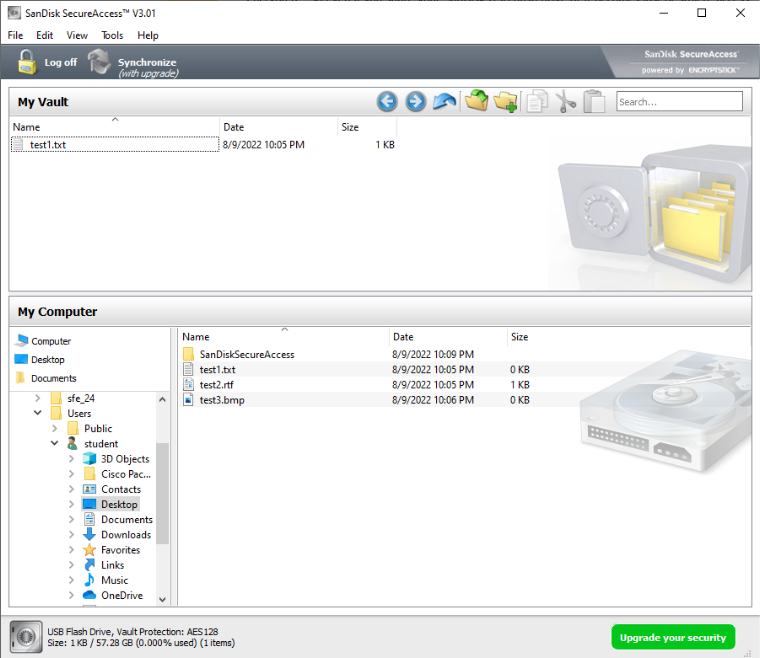
**The Simplest Backup For Your Important Data - USB Flash Drive**  
  
 Author: Landon Kea  
  


**What is a Backup?**

A backup is a copy of a data file that is stored in a separate location from the original data file. In the case of a data loss event, the backup file may be used to restore the lost data.

This backup file may be used to restore the original after a data loss event.

**Why We Backup?**

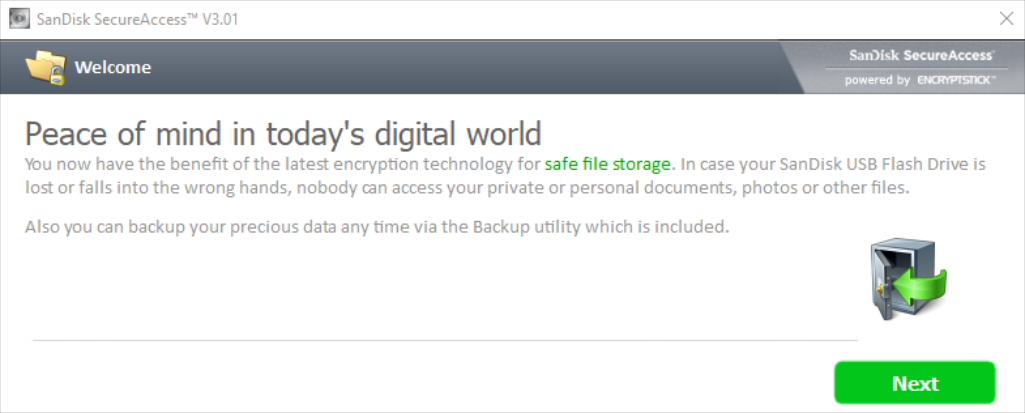
Backups are ALWAYS necessary. The primary reason to create a backup is to recover data after its loss. The loss can occur by accidental deletion, a virus attack, or a software or hardware failure. If any of those things occur and the files are backed up, those files can easily be restored from the backup. Having a backup is mandatory for any person or organization concerned with their information.

**Backup Considerations:**

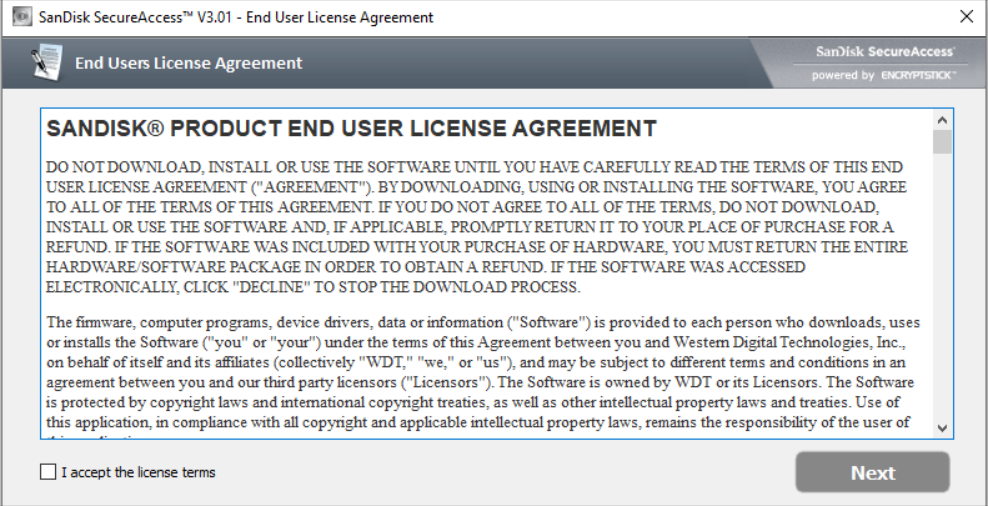
Method of backup, choosing the best backup option, what to backup, frequency of backing up, location(s) of storing the backup, security, and retention.

**How to Backup Important Files with a Sandisk USB Drive in Microsoft Windows:**

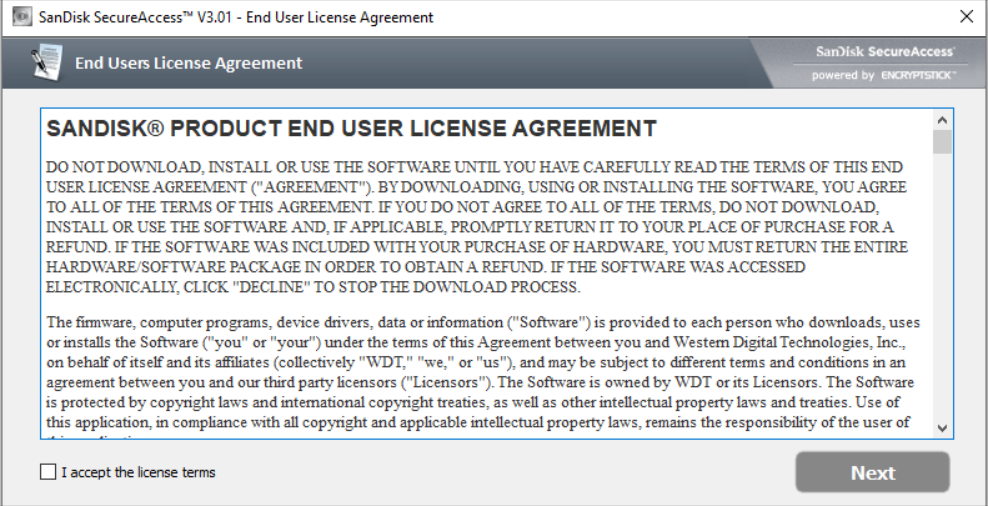
1. Plug the USB drive into a Universal Serial Bus (USB) port on a computer running the Microsoft Windows Operating System.
2. Double click on S**anDiskSecureAccessV3.01\_win.exe**



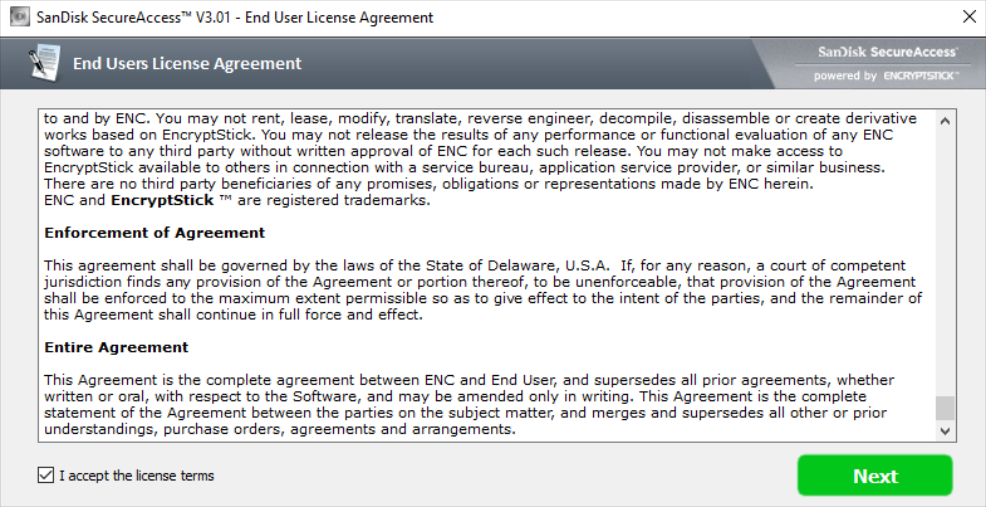
3) This will open the window shown above. Click the **Next** button in the lower, right hand corner.



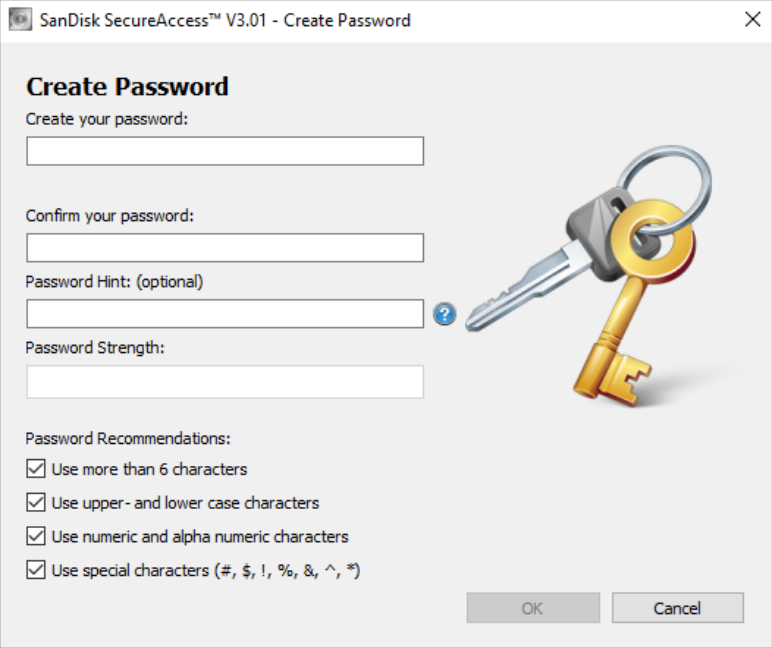
4) Read through the entire end user license agreement by using the scroll wheel on the right side and scrolling down.



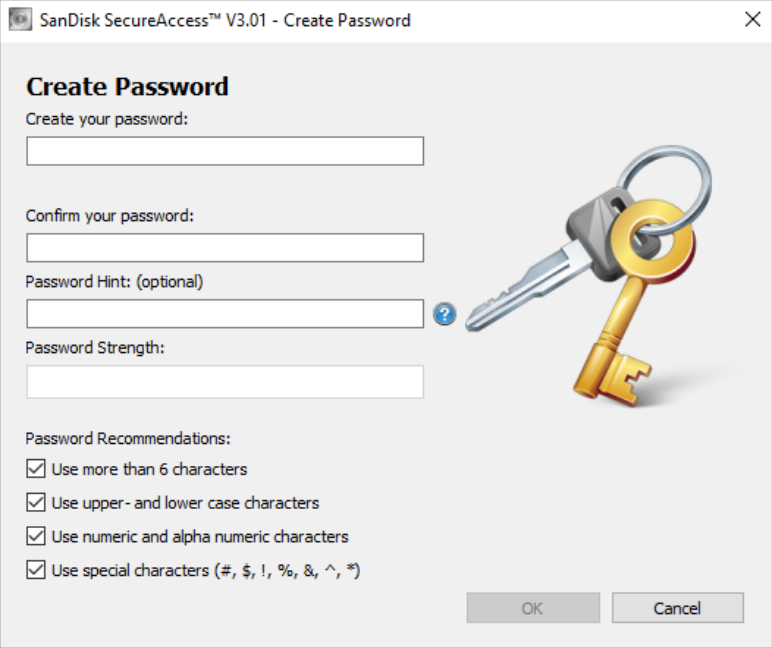
5) After everything is read through and understood, then click on the check-box that says “**I accept the license terms**” in the bottom, left hand corner.



6)Click the **Next** button in the lower, right hand corner.

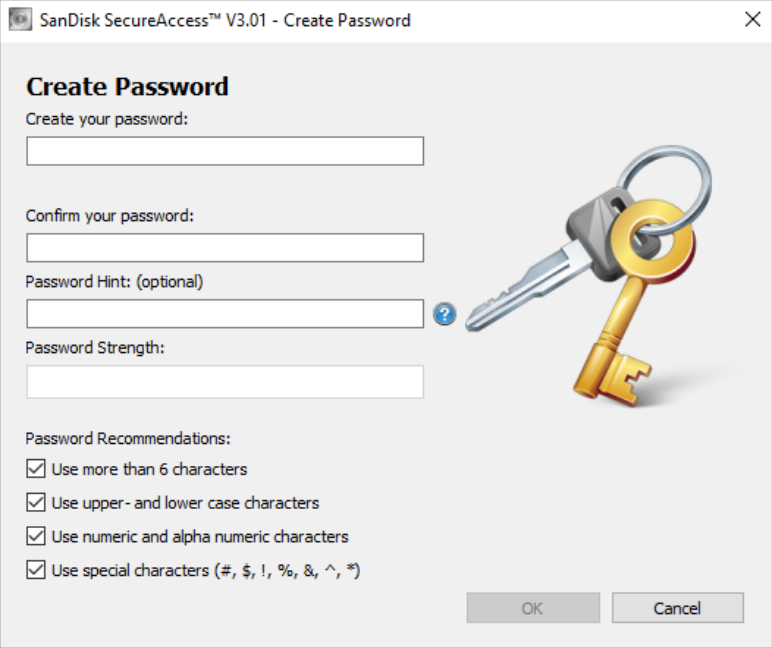


7) Under the “password recommendations”, remove all checks in the check-boxes.

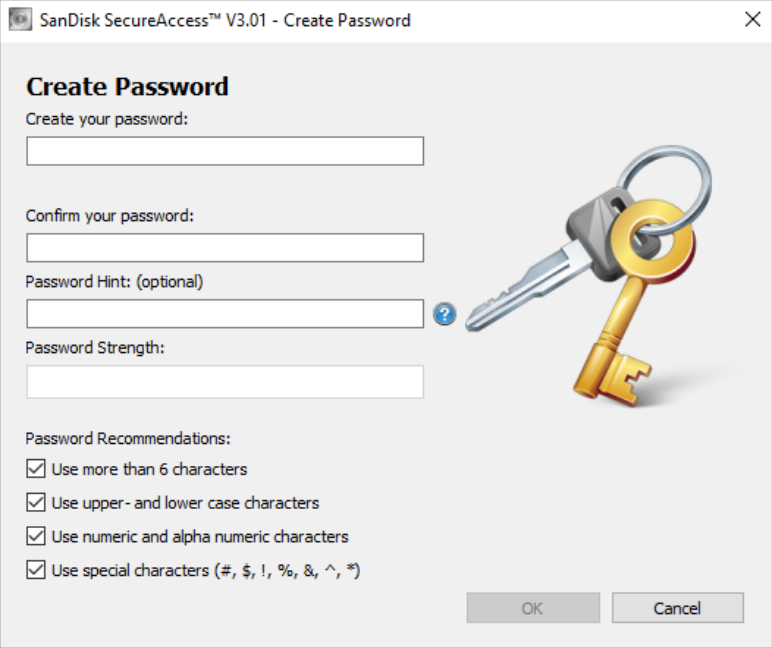


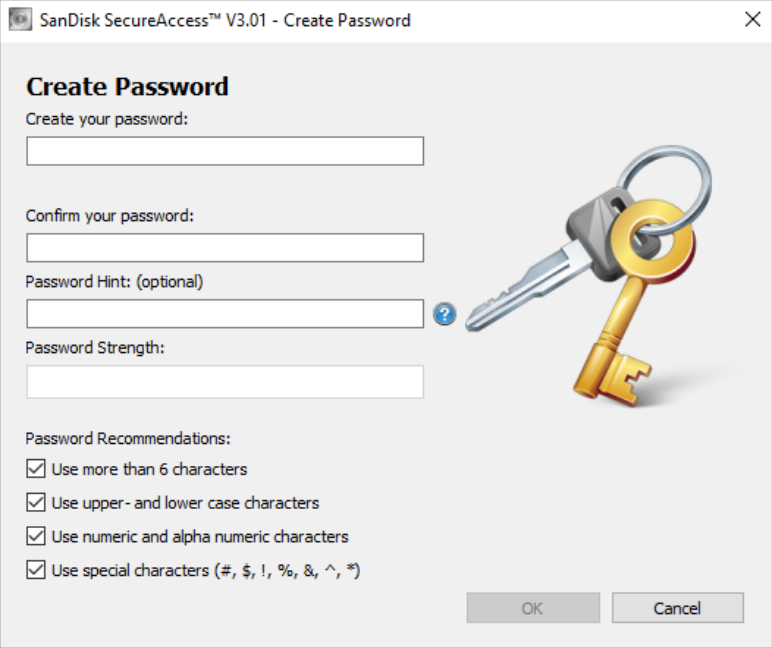
8) In the create your password: box, type a passphrase that you will not forget.

[Note: A password is a short character set of mixed digits. Although a passphrase is a longer string of text that makes up a phrase/ sentence. A passphrase in general is a phrase made up of at minimum **three** different and unique words. This passphrase is able to contain numbers, Uppercase and lowercase.]

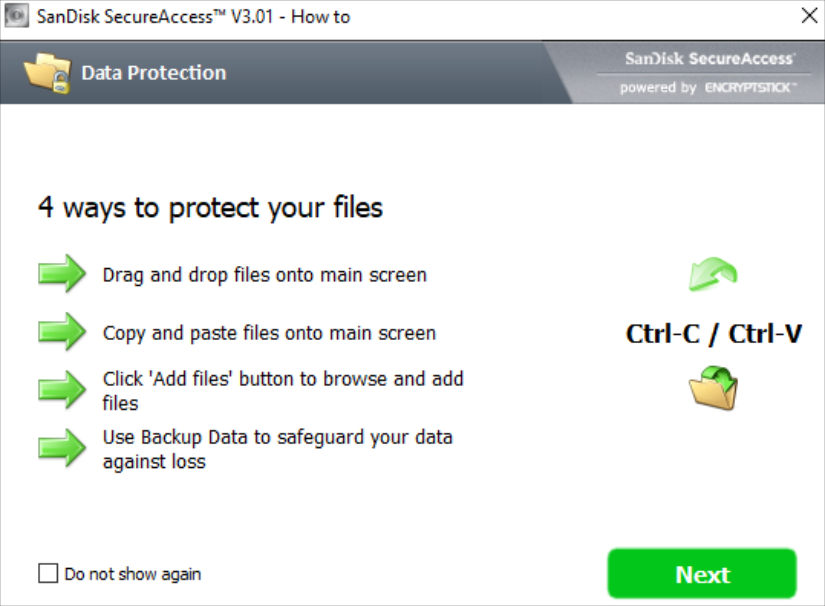


9) Retype the password to confirm.

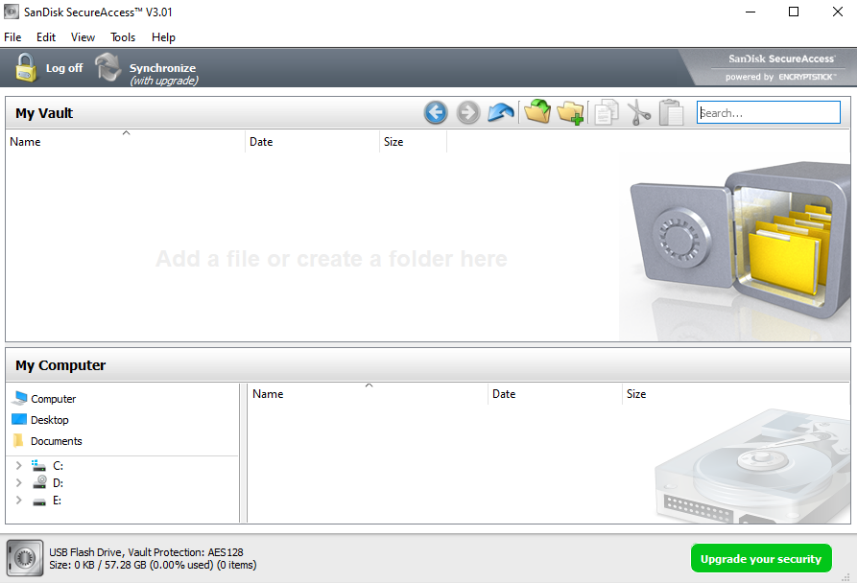
  
  
  
  
  
  
  
10) Fill out the password hint.



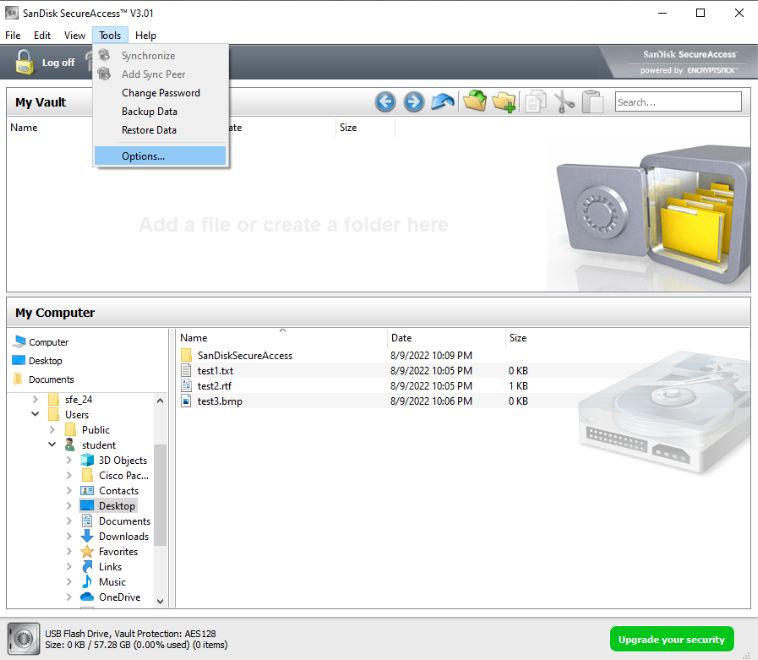
11) Click the **Ok** button in the lower, right hand corner.



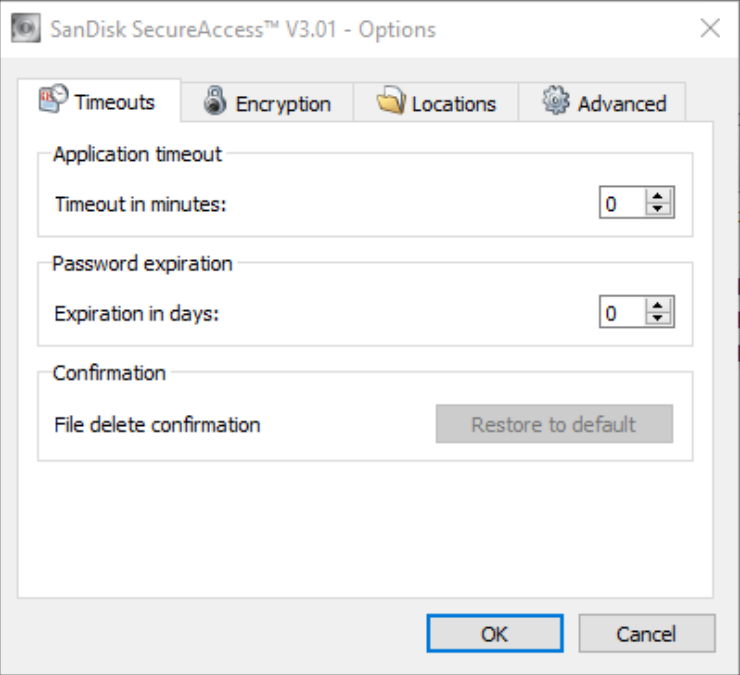
12) On the list of possible options, click **Next**.



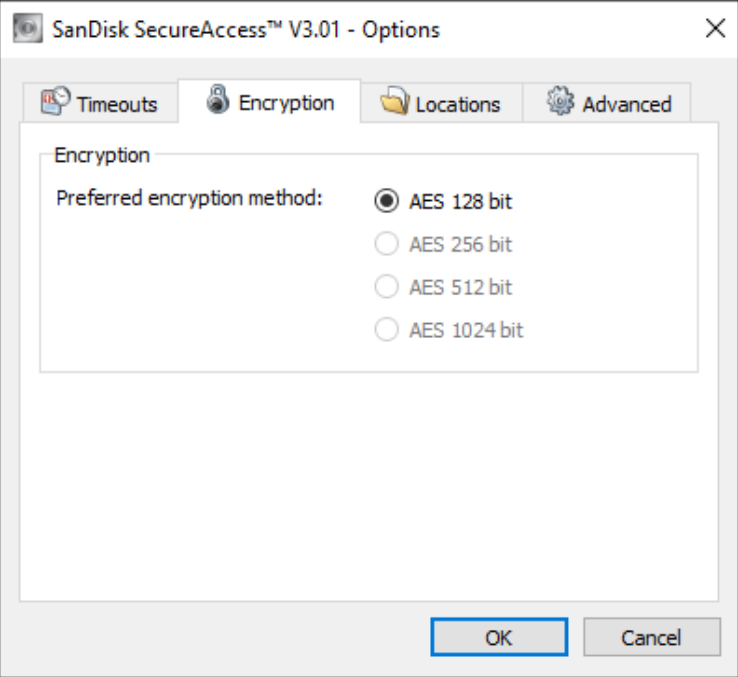
13) This is the main page for the tool.



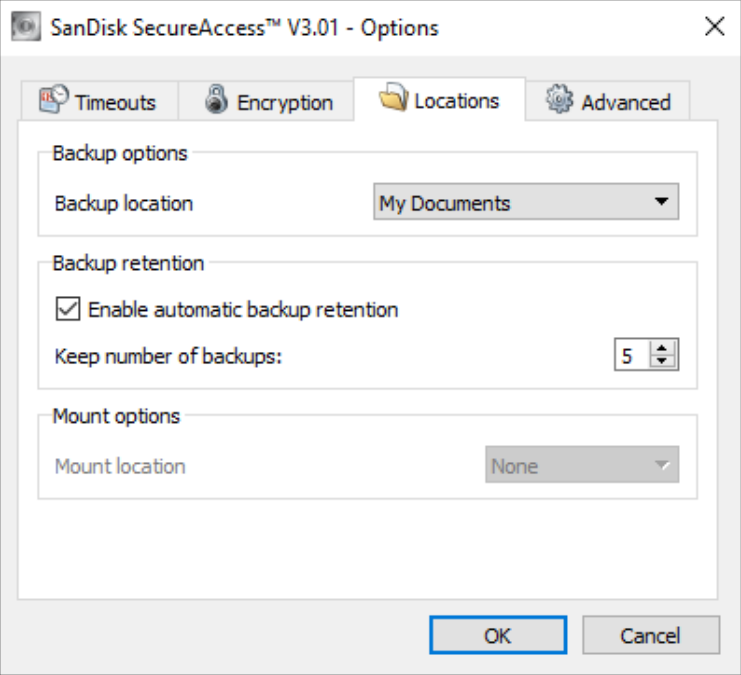
14) Click on **Tools** in the **header** and select **Options**:



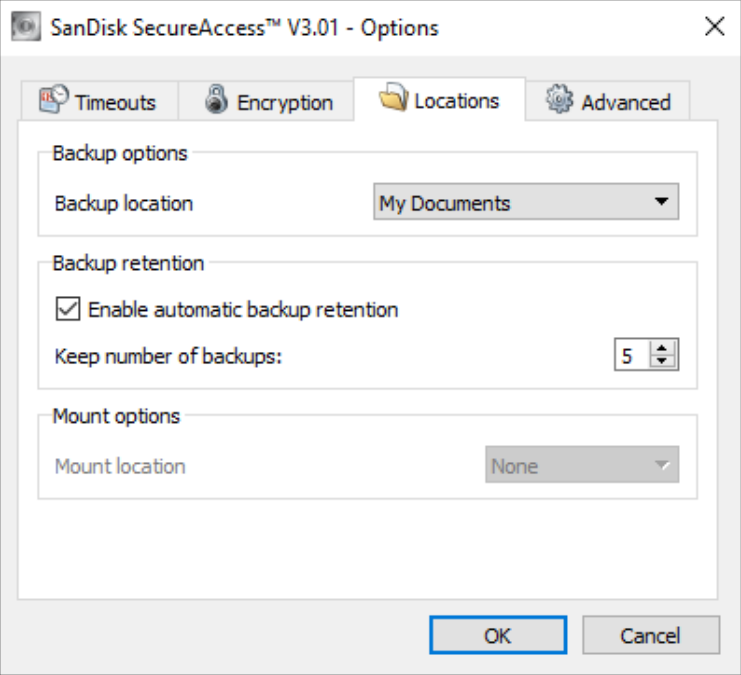
15) Verify under the Timeout tab is zero minutes and zero days.



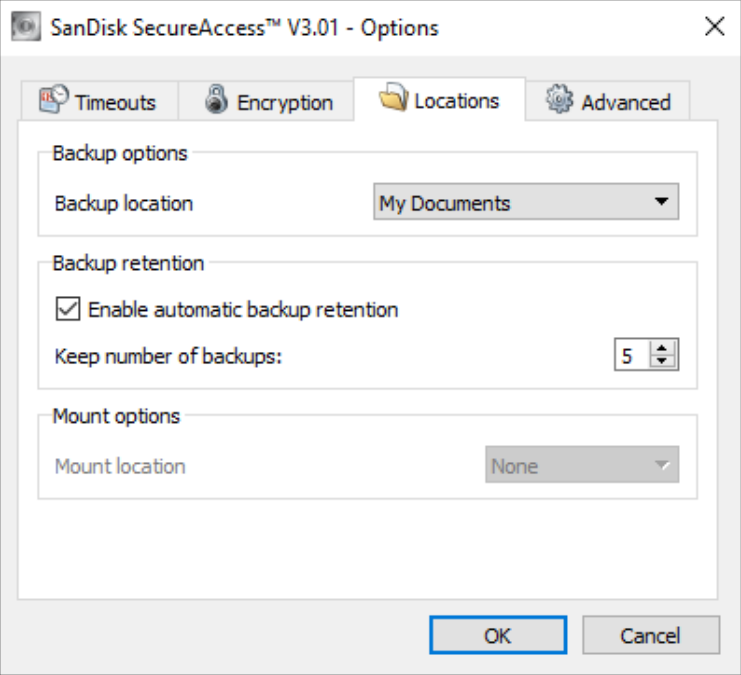
16) Verify under the Encryption tab AES 128bit is selected.

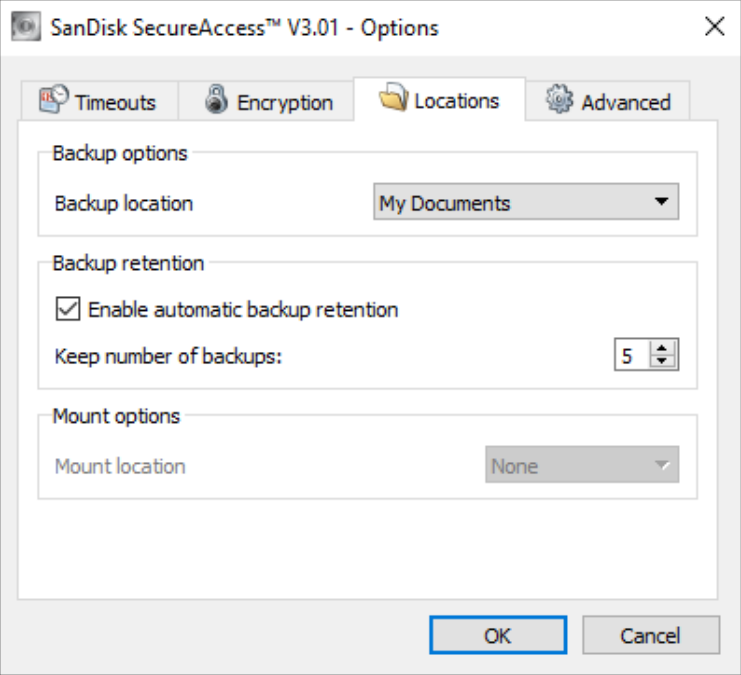


17) Under the Locations tab, locate the Backup options box. For Backup location make sure the drop down “My Documents” is selected.

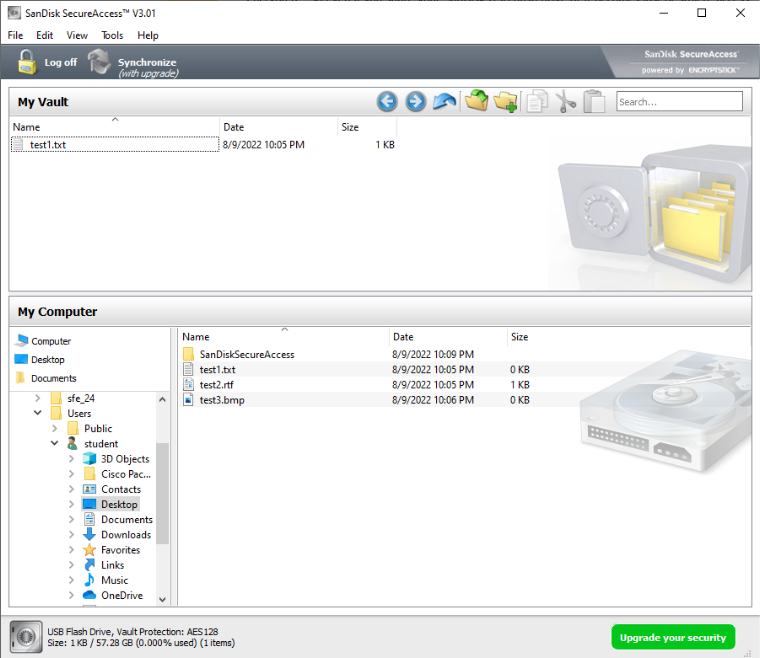


18)Check the box that states “Enable automatic backup retention”.



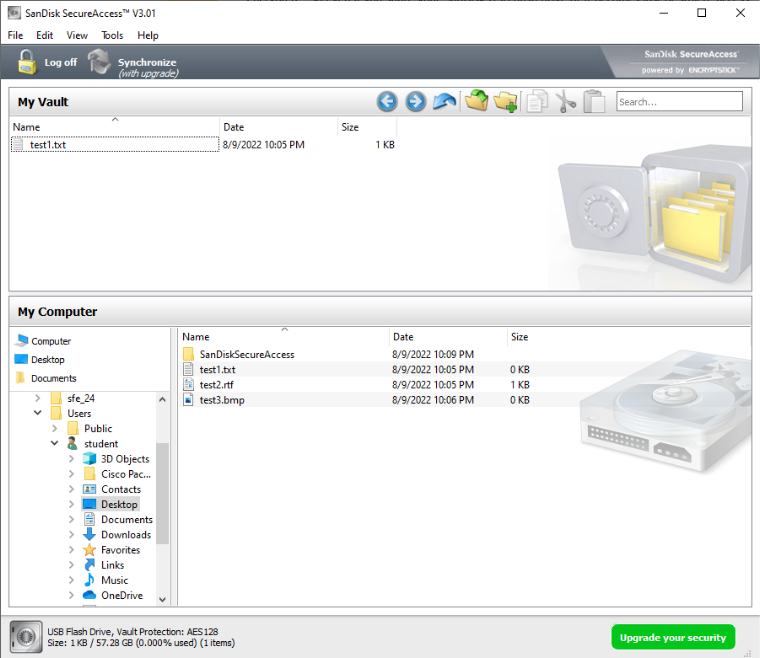
19) Increase the number of backups to the maximum backups to larger than 5.  
  


18) Click the **Ok** button in the lower, right hand corner.

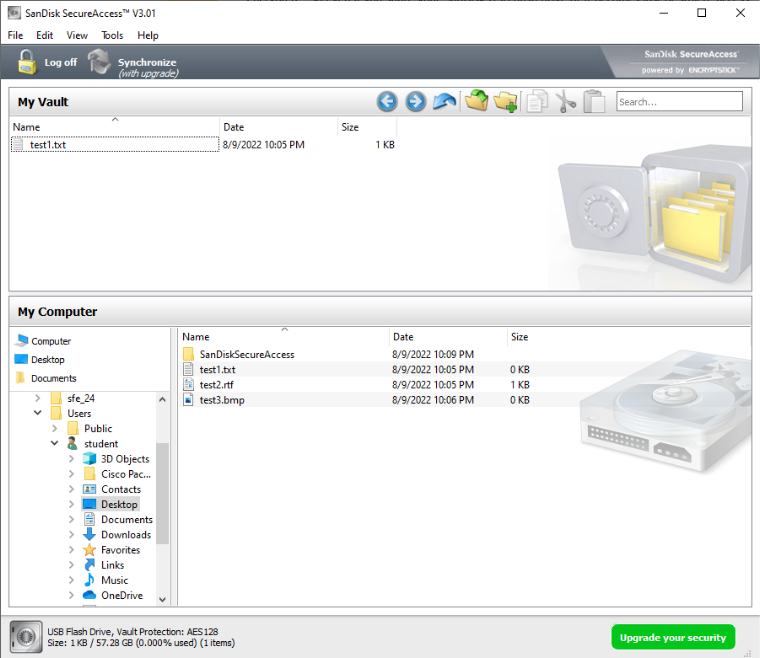


19) On the left navigation pane, find the files that are to be backed up.

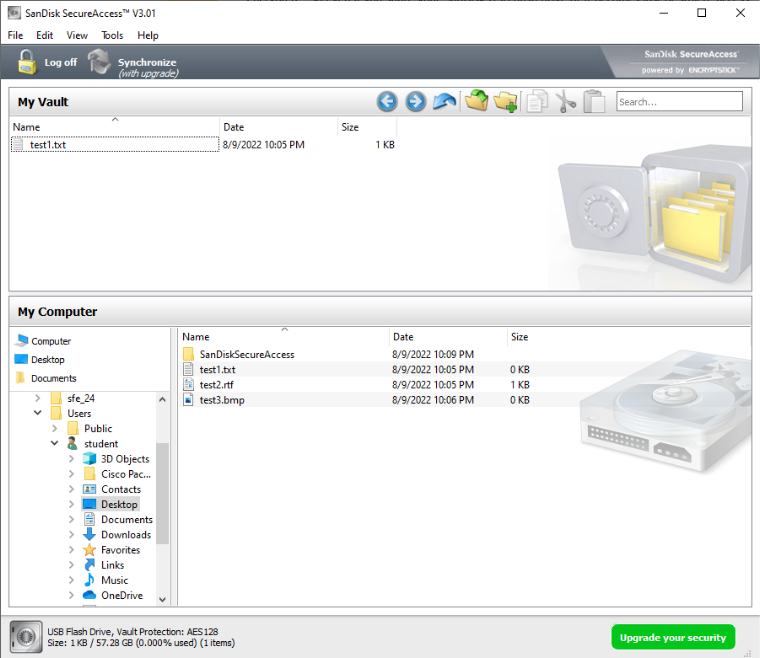
*Note: Priceless, sensitive, or otherwise irreplaceable pictures and important documents should be considered for backup.*



20) Drag and Drop from down below to the section where it states “My Vault”.



You can also select the icon to import files into the vault:

  
  
  
21) Once that is done, click on Tools in the header and click backup.

**Other Backup Methods:**

There are multiple methods of storing backup data. You can setup regular backups of data in-house (locally), or via an external service (vendor). There are also software packages (free and purchased) that can be used to backup data. In either case, wizards typically guide you through the process of setting up your backup, and include things such as designating the destination device for your backups, choosing the folders/files to be backed up, and specifying the frequency of backup. Keep in mind that if you use any of the non-cloud-based destination options for your backup data, it is advisable to keep a copy of the backup device contents in a secured location separate from the office.

The following are possible methods of storing backup data.

***(1) Removable Storage Media***

Storage media that you can connect to and disconnect from your computer are a more versatile backup option than your computer’s internal hard drive. Physically separating your backups from your computer helps keep your data safe, both from online attackers and power surges.

*Pros of using Removable Storage Media:*

Removable media are a flexible data storage alternative because most are portable and work on most computers. They are also available in a wide variety of storage capacities and prices, so you can find the device that fits your needs and budget. Most removable media are also reusable.

*Cons of using Removable Storage Media:*

Portability makes removable storage devices convenient but also makes them prone to loss or theft. Rolling backups may spread corruption and malware from the primary files to the backups.

*Security:*

Unlike remote storage, removable storage media give you direct control over your data. However, that means you are responsible for protecting that data, especially when traveling with it. To increase the security of your removable media devices, password-protect them; encrypt their data when possible; connect them only to systems that follow network security recommended practices, such as the use of firewalls and antivirus; remove them from the computer when you complete your backup; and secure them physically.

*Types of Removable Storage Media*

*External Hard Disk Drives:*

External hard drives are the same as internal hard drives, but they are portable and easy to install. They are prone to physical damage and degaussing, and they are bulkier than solid-state storage of similar capacity.

*Solid-State Storage:*

Unlike hard drives, solid state devices contain no moving parts, which allows them to be small, resist shock, and access data quickly. USB drives are small enough to slip into a pocket and are plug-and-play compatible with most computers. Solid state media are rewritable, though they do not store data magnetically and so are not in danger of degaussing. Writing data to a solid state device will eventually wear it out, though modern device controllers extend media lifespan. Many SSDs and even USB drives now come with built-in password protection and data encryption. The small size of these drives make them easy to lose, so it is best to always keep track of their physical location.

***(2) Remote backup with external cloud storage:***

Cloud storage is a service model in which data is stored remotely and made available to users over a network (typically the Internet). It enables you to store your files online with the ability to access and share them from any computer connected to the internet. The files are kept on an external server, and the hosting company makes them available to you online. It offers great convenience, but security and cost are potential concerns. Many cloud storage options (such as Dropbox, SkyDrive, Google Drive, etc.) work by staying synced with a dedicated folder on your hard drive.

*Pros of Cloud Storage:*

Remote backup services can help protect your data against some of the worst-case scenarios, such as natural disasters or critical failures of local devices due to malware. Additionally, cloud services give you anytime access to data and applications anywhere you have an internet connection, with no need for you to invest in networks, servers, and other hardware. You can purchase more or less cloud service as needed, and the service provider transparently manages your resource usage as it grows or shrinks. Some providers can also ensure regulatory compliance in the handling of sensitive data, which may benefit small businesses.

*Cons of cloud storage:*

The cloud’s dependence on the internet can delay communications between you and the cloud. In addition, there are no universal standards, platforms, or languages for cloud computing, so you may become locked into one provider. The physical distribution of cloud data over many geographically dispersed servers may cause some organizations, especially ones handling sensitive data, problems with jurisdiction and fair information practices. Cloud customers have little or no knowledge of their service provider’s cloud infrastructure or its reliability, and users surrender most of their control over their own data.

*Security of cloud storage:*

Cloud service providers can often encrypt user data, making it harder for attackers to access critical information. However, cloud users have little or no direct control over their data or knowledge of their cloud service provider’s security practices. Shared clouds store your data along with many other users’ data in the same cloud infrastructure, posing a security risk. Before you entrust your critical data to a cloud service provider, carefully check the service agreement for security practices. To increase the security of your data in the cloud, look for a cloud service provider that will encrypt your data with established encryption algorithms, such as Advanced Encryption Standard (AES) or Blowfish; transfer your data via a secure socket layer (SSL) connection; follow established network security recommended practices, such as the use of firewalls; physically protect the hardware that stores, processes, and transmits your data; and prevent your data from leaking to other customers on its cloud.

*Cloud Storage Options:*

Below is a list of some popular cloud storage options. Most services are free up to a certain number of gigabytes. After that, prices vary by the number of gigabytes stored.

[*https://nextcloud.com/*](https://nextcloud.com/)

<https://www.dropbox.com/>

<https://www.box.com/>

<https://www.amazon.com/clouddrive>

<https://www1.sugarsync.com/>

https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage

***(3) Vendor-Managed Backups:***

A backup service is another option where you pay companies that specialize in performing

backups for you. Your data is stored on servers they own. Restoring data from a backup service is significantly slower than a local backup since your data is in another location. Also, costs of this service and security of your data must be considered when choosing this option.

*Considerations when using a Backup Service:*

Before storing any files on someone else’s server, make sure that the hosting organization is

legitimate. Do they really host files? Do they have a reputable name? Also it is important to

make sure the organization is trustworthy. Are the files only available to you? Or are they

available to everyone? Last is the organization reliable. In the event of a catastrophe, will the

backed up files be available to you? Are their servers ever down?

*Security:*

It is important to carefully examine any contracts with the off-site backup provider. This is

because another entity will have the actual possession of some of the most valuable assets to

your organization. This is why it is mandatory that your organization seek audit rights, and

assurance that the company’s hiring procedures include thorough background checks. Your

organization must do everything in its power to ensure the safety of all assets. It is also important to make sure that your organization uses locked containers to transport and valuable assets or information such as backup data. Locks will discourage some threats and also prevent another customer from inadvertently loading your information onto their own

system.

*Vendor-Storage Options:*

Below is a list of some backup services.

https://spideroak.com/

<https://proton.me/>

<https://www.carbonite.com/>

https://cyberfortress.com/

***(4) Internal hard disk drives:***

Hard disk drives store data on a spinning magnetic platter read by a moving read/write head. Nearly all desktop and laptop computers use their internal hard drive to store most of the information they need in order to run, as well as the user’s working, primary files. Secondary systems and backup servers also store data on internal hard drives.

You can buy hard drives in a wide range of storage capacities, from a few dozen gigabytes of

data to several terabytes. Because hard drives are rewritable, you can use them

to perform rolling backups, a method that automatically and periodically updates the backup files with the most recent versions of the primary files.

*Pros of using Internal Hard Disk Drives:*

Keeping primary file copies and backup copies on the same internal hard drive allows you to

quickly update backup files and maintain a simple file structure.

*Cons of using internal hard disk drives:*

Rolling backups can silently propagate any corruption or malware in the primary files to the backup files. Worse, if your internal hard drive is damaged, stolen, or corrupted, you could lose both your primary and backup files. In addition, your computer constantly uses the internal hard drive, so the more backup files you store there, the less space your computer has to operate. Lastly, the working lifespan of hard drives varies, and installing new internal hard drives requires some technical expertise.

*Security of using internal hard disk drives:*

Backup files stored on the internal hard drive are just as vulnerable to damage and corruption as the primary files. Additionally, internal hard drives are only as physically secure as the computers that house them. You can encrypt hard drives to prevent unauthorized access to stored data, but data can be erased—and the hard drive rendered unusable—via magnetic degaussing without accessing the drive electronically. To increase the security of your internal hard drive, encrypt the drive’s contents, physically secure your computer, and follow network security recommended practices, such as the use of firewalls and antivirus.

*The methods in the next few paragraphs are used very rarely.*

***Optical Storage:***

Optical storage media, such as compact discs (CDs), digital versatile disc (DVDs), and Blu-ray discs, store data on reflective discs read by a moving laser head that can also write data onto rewritable discs. Storage capacity varies greatly among the available optical media, from 682 megabytes on CDs, to as much as 9.4 gigabytes on DVDs, to up to 50 gigabytes on Blu-ray discs. Non-rewritable discs do not allow for rolling backups, so they might not contain the most recent version of primary files. However, data on non-rewritable discs cannot be accidentally erased or inherit corruptions or malware from later versions of primary files. Optical discs are also relatively inexpensive, though they do not come with built-in data encryption, so a third-party solution would be required. Optical discs, especially CDs and rewritable discs, do not last forever. Handling can shorten their lifespan and, short of multi-disc hardware, optical discs must be individually handled.

***Magnetic Tape – note this is stable and will be seen in large corporations but is usually not used in small office home office locations:***

A digital tape system comprises a tape deck, individual tapes, and, optionally, a tape auto-loader. Individual digital tapes can provide capacities of more than a terabyte, or roughly a thousand gigabytes, and are fairly cheap. Once installed, digital tape systems require little user interaction and access data very quickly. The reusable tapes enable rolling backups but are less vulnerable to viruses than hard disks, if older versions of files are adequately archived. The many different brands of digital tape systems are not all compatible, making it harder for you or, on the plus side, thieves to use your tapes in different systems.

***Floppy or ZIP Disks – note this is no longer used as storage amount is too small:***

Floppy disks and ZIP disks store data on spinning magnetic platters, much like hard drives. However, their storage capacity is extremely low compared to other storage media, and the drives that read them are no longer being produced, making floppy disks and ZIP disks obsolete.

**Choosing the best backup option:**

Before you choose a data backup option, assess the advantages and risks of each media, your financial resources, and your needs, such as the amount of data to be backed up, protection for sensitive data (customer data, personally identifiable information, or personal health information), and accessibility of data (permanent archiving, temporary backups, and rolling backups). Home users storing a relatively small amount of personal data should consider keeping primary files on the hard drive of their computer, with at least two backup copies on solid-state storage, optical storage (stored in jewel cases), or remote storage. Individuals or small businesses who want to store large amounts of non-sensitive data should

consider keeping working files on their hard drives or servers, with at least two backup copies on separate servers, high-capacity optical media, high-capacity solid-state storage, digital tape systems, or cloud storage. If the stored data is sensitive, be sure to carefully consider the risks of cloud storage, encrypt your data, and keep any storage media physically secure.

Large businesses or organizations should consider keeping one backup copy onsite and another offsite either through a separate data service (such as a cloud service provider or remote server backup) or on the organization’s own off-site servers or digital tape system.

Whatever backup options you choose, remember to follow the 3-2-1 rule of backups:

3 – Keep 3 copies of any important file: 1 primary and 2 backups.

2 – Keep the files on 2 different media types to protect against different types of hazards.

1 – Store 1 copy off-site (e.g., outside your home or business facility).

**What to Backup:**

Data and applications that would be rather hard and cumbersome to replace such as tax and accounting paperwork. Also priceless, sensitive, or otherwise irreplaceable pictures and important documents. It is important that organization information be backed up whether it resides in the office, and/or on any home computers that people may be working on for office work.

**Frequency:**

Backups must occur regularly in order to prevent data loss. Individual computer users can back up their own information when desired and using methods they desire, whereas data on organization servers need more formal backup procedures. For organizations, the more backups that take place, the better.Frequent backups take time, money, and resources but the benefits outweigh these negatives.

**Storage Location:**

It is a good practice to keep some backup information off-site. In the event

that a natural disaster occurs, your backup will mean nothing if it got destroyed with all the

computers and the building.

**Security:**

Security attacks, whether in the form of malicious Internet content, theft of physical devices, login violations, or denials of service (meaning others are prevented from accessing your site) can catch you off-guard and unprepared to deal with them once they occur. Therefore, whether your backup data is onsite or offsite, you will want to ensure the backup information is secure and accessible only by those authorized to use it to restore lost data. Encryption of data is the process of transforming information to make it unreadable to anyone except those possessing special knowledge. Encryption must take place with any valuable information, including sensitive information in backup data. Not every piece of information should be available to and easily readable by the public. Some data is sensitive and should be protected for safety and privacy reasons. In order to use encrypted data later on (e.g., if you need to use your encrypted backup data to restore your system after a failure), the data must be decrypted. Decryption is the process of restoring encrypted data to a readable format.

**Retention:**

The amount of history to be saved is another thing to consider. You may want to keep backups that are years, months, weeks, or even just a day old. Keep in mind that the more backups you wish to save, the more space you will need to have and this will include increased costs. Some organizations may be legally obligated to keep 1, 2, 3, or more years of history for their business.

**Summary:**

All computer users, from home users to professional information security officers, should back

up the critical data they have on their desktops, laptops, servers, and even mobile devices to

protect it from loss or corruption. Saving just one backup file may not be enough to safeguard

your information.

Backup Steps: The Basics

1. Find the files that you want to backup (documents, spreadsheets, databases, etc.)

2. Copy the files to backup media (USB Drive, external drive, cloud storage drive, etc.)

3. Repeat above at scheduled frequency

Note: this is a rudimentary level of backup. Ideally, you should keep your files organized

in folders for easy identification of files needing backup.

Some content under “Other Backup Methods:” sourced from:

**Data Backup Options** by Paul Ruggiero and Matthew A. Heckathorn

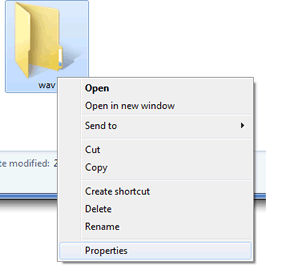
<https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf>

**Manually encrypt of file and folder via Microsoft Windows:**

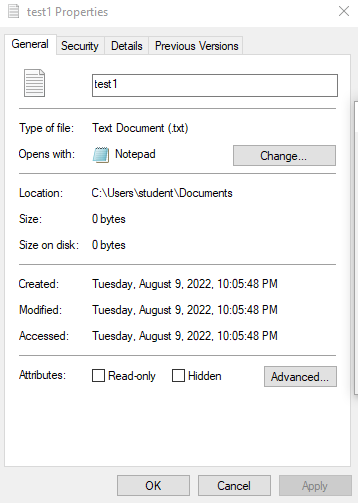
Steps to Encrypt a file or folder:

These are instructions are for Windows:

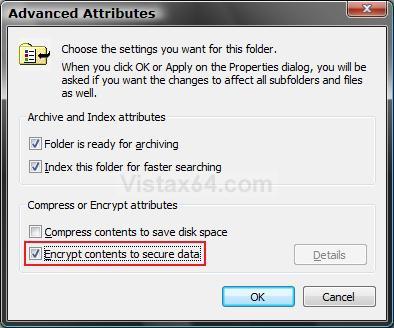
1) Right-click the folder or file you want to encrypt, and then click properties.



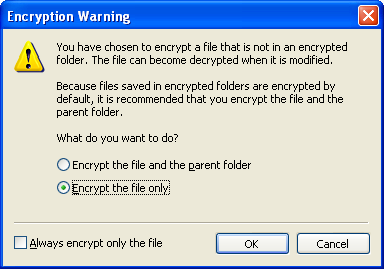
2) Click on general tab, and then click advanced.



3) Select the encrypt contents to **secure data check box**, and then click **Ok**, and click **Ok** again to exit the properties windows.

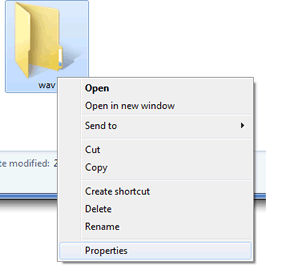


4)If you are encrypting a file and get an encryption warning, click the button to encrypt the file only, then click **Ok**.

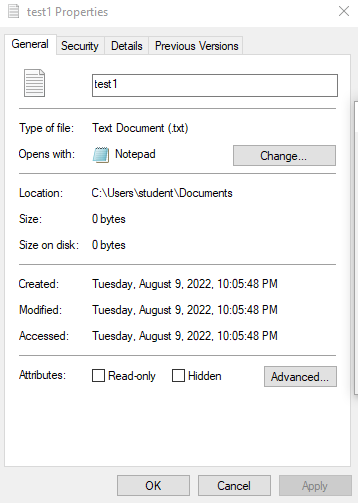


Steps to decrypt a file or folder:

1) Right-click folder or file you want to decrypt, and then click properties.



2) Click the general tab, and then click advanced.



3) Click the encrypt contents to secure data check box to remove the check mark that was previously there, and then click **Ok**, and click **Ok**, and click **Ok** again to exit the properties window.

