# Infotip – Encrypting files on OSX

Use this InfoTip to encrypt files on OSX. Encrypted files can only be accessed by inputting the proper password. This is a good way to ensure the contents of the files are kept private and secure.

Please remember that encryption process in OSX uses the specified folder and makes a duplicate of that folder that is encrypted. The original folder and its contents will still be unencrypted, and available for use.

## Prerequisites:

* Encrypted files in OSX are saved as a .dmg file. This file type acts as an external, mountable drive (like a USB drive).
* Encrypted files are **NOT** cross platform. (i.e.: Windows machines will not recognize a .dmg file)
* Encrypted files are **NOT** backwards compatible and cannot be viewed in previous OSX operating system versions (i.e.: a file encrypted in OSX High Sierra will only be viewable in High Sierra and newer OS versions. Sierra and older OSX operating systems will not be able to access the file)

**Recommendation:**

* If saving to a USB drive, please remember that USB drives are not recommended to be used as a backup drive for file storage. They should be used to transport files only. Please use a proper backup application if you need to backup and store files.

**Procedure**

1. Open the Disk Utility application (command + space will open up Spotlight and allow you to search)
2. Click on File > New > Image From Folder



1. Select the folder you want to encrypt
2. Select the level of encryption. Default is a faster, but weaker encryption. It is recommended to always use a stronger form of encryption (256-bit AES in this case) however this will increase the amount of time needed to encrypt and decrypt.
3. If you want the folder to be editable, choose read/write in the Image Format



1. You will be prompted to choose a password. Pick a strong password: at least 12 characters and use upper and lower letters, numbers and special characters.



1. **Do not forget this password.** If you forget this password, you will **NOT** be able to access the folder and the encrypted data will not be recoverable.
2. Store your password. We recommend using a password manager application to ensure you don’t lose your passwords.