SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-GDL-009-M10 – Encrypting Personal Computers (Mac OSX)

Author: Paul Ferrier

Date: 11/10/2016

Document Security Level: **PUBLIC**
Document Version: 1.2
Document Ref: SEC-GDL-009-M10
Document Link:
Review Date: 01/10/2017

SEC-GDL-009-M10 – Encrypting Personal Computers (Mac OSX)

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	24/06/2016 15:20			
1.0	PF	ESA	Updated the document following peer review	11/10/2016 08:10			
1.1	PF	ESA	Consolidated document to cover OSX 10.7 – OS 10.12	12/10/2016 07:35			
1.2	Richard Brown	ESAA	Finalised document ahead of publication	25/10/2016 16:00			

Contents

SEC-GDL-009-M10 – Encrypting Personal Computers (Mac OSX)

1. Introduction

Details on how to enable encryption on **Mac OSX devices from version 10.3 to 10.6** using **File Vault** are located here https://www.securemac.com/osx/mac-os-x-filevault-review-encrypting-files-and-folders, this document focuses mainly on **File Vault 2** and how to operate it.

Versions of **Mac OSX 10.7 (Lion) through to and including Mac OS 10.12 (Sierra)** offers users the ability to protect their files and folder with full disk encryption using **File Vault 2**. This means that if the hard drive is taken out of the computer either a password or a software key are required to be able to access the data. These guidelines focus on these versions of the operating system.

Encrypting devices does not make them exempt from the DPA or the FOI act and hence you must be able to comply with the requirements to provide information, or the encryption key if required.

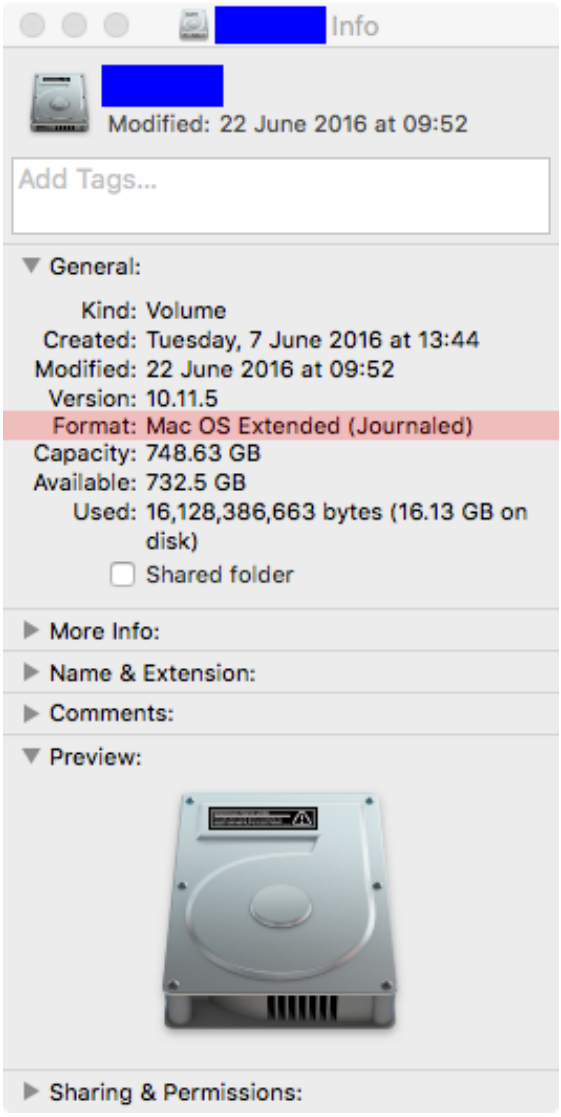
One word of caution, if you lose your encryption password or recovery key your data will be inaccessible.

These guidelines provide the steps required to encrypt (and decrypt if required) a personal computer.

2. Quick check on drive encryption

If you need to quickly check whether your computer is encrypted there are two ways to check:

2.1

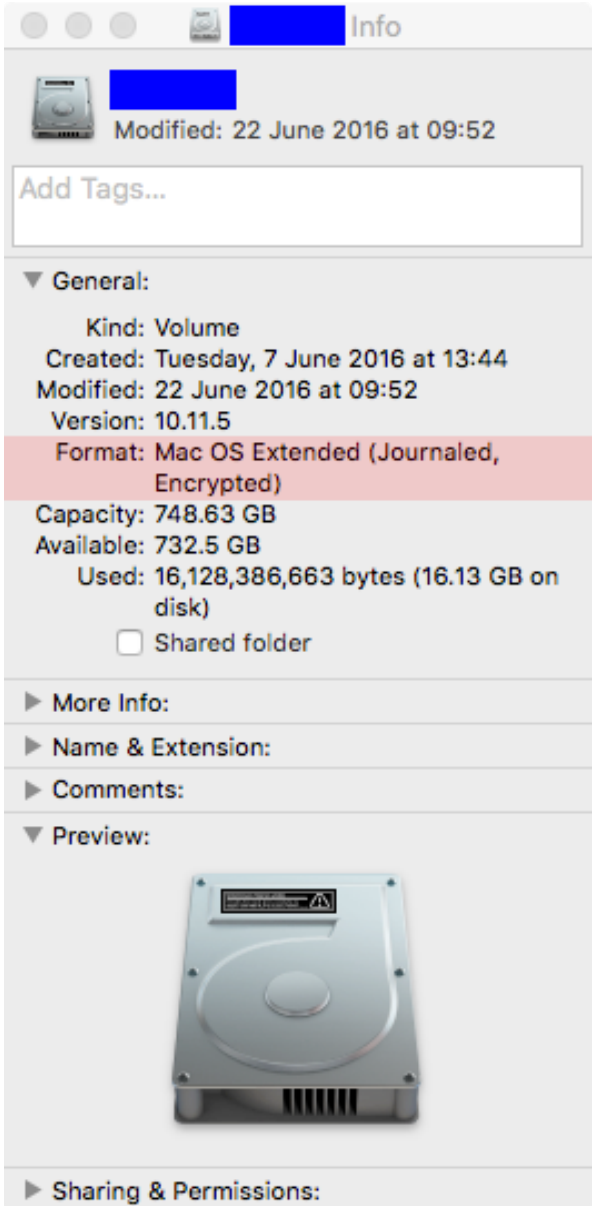


Using the Info on the hard drive, right click on the drive in question and select "Get Info" Highlighted in the picture on the left you will see that the format of the hard drive does not include the any encryption details.

In this instance the hard drive is not encrypted.

Please see section 2.2 to see the equivalent encrypted hard drive version of the quick check.

2.2



Highlighted in the picture on the left you will see that the format of the hard drive has an encrypted hard drive.

2.3 The other option is to look in **System Preferences** at the **Security and Privacy** item.

You will be presented with the screen provided at the start of section 3 – Encrypting a drive.

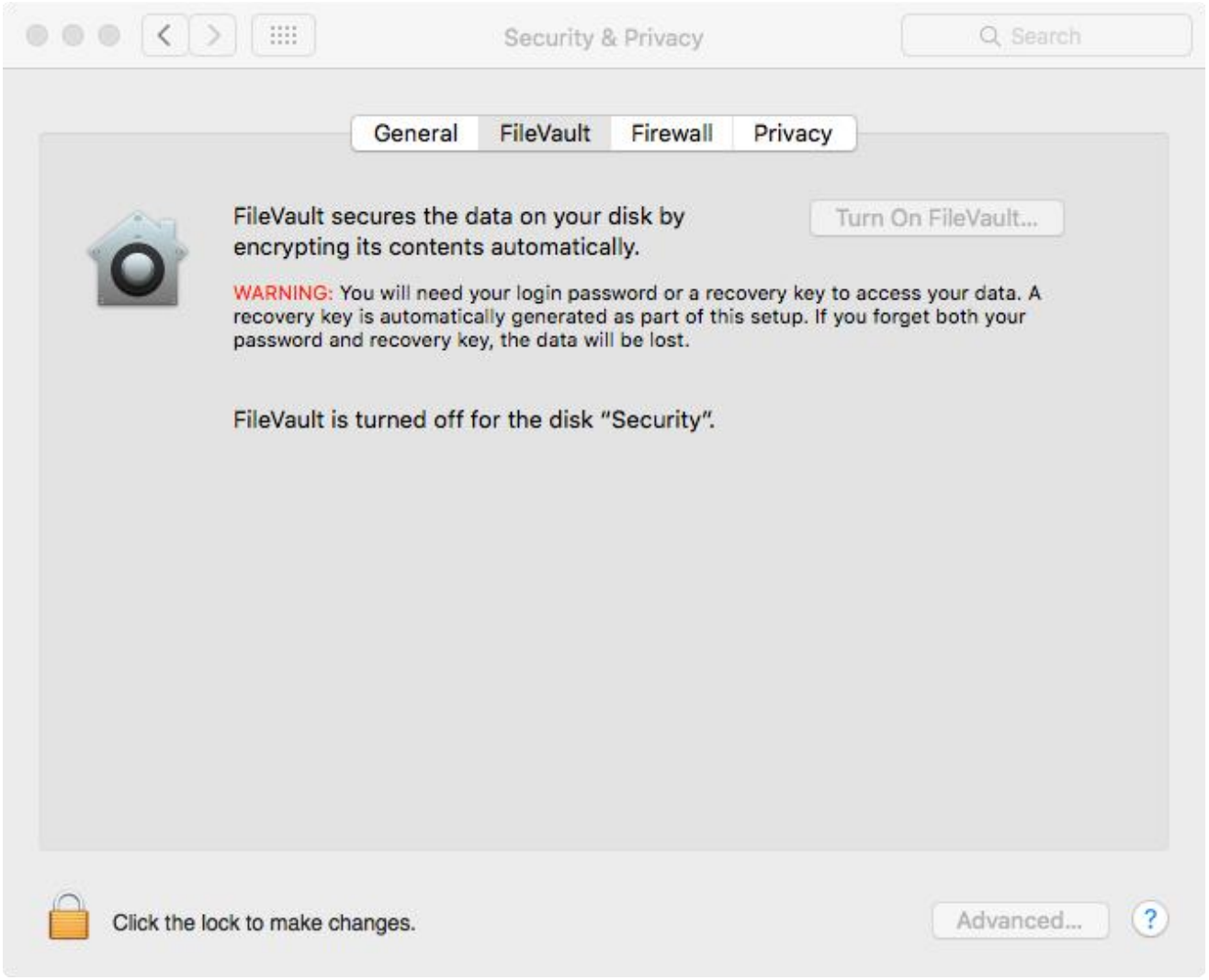
3. Encrypting a drive

By default, you will see the Turn On FileVault option greyed out, if the padloack on the bottom left hand corner of the window is closed. Click this and provide your username and password to allow the Turning on of FileVault.

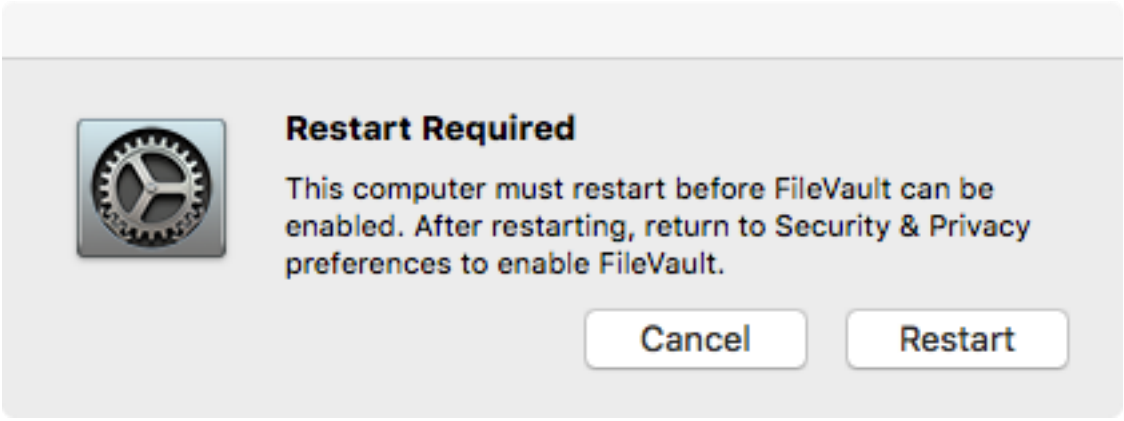
Please note you can use this process to encrypt any external (or internal) hard drive in your Mac, you could encrypt USB drives using the same process. Please be aware though, that if you use both a Windows PC and a Mac then while you can mount your encrypted drive on a PC, it will only mount in a read only format.

IMPORTANT

Before you start the encryption process, it would be worth backing up any files and folders that are really significant. This is not to say the the encryption process or hard drive would fail during the process, but it provides a safety net should it be required.



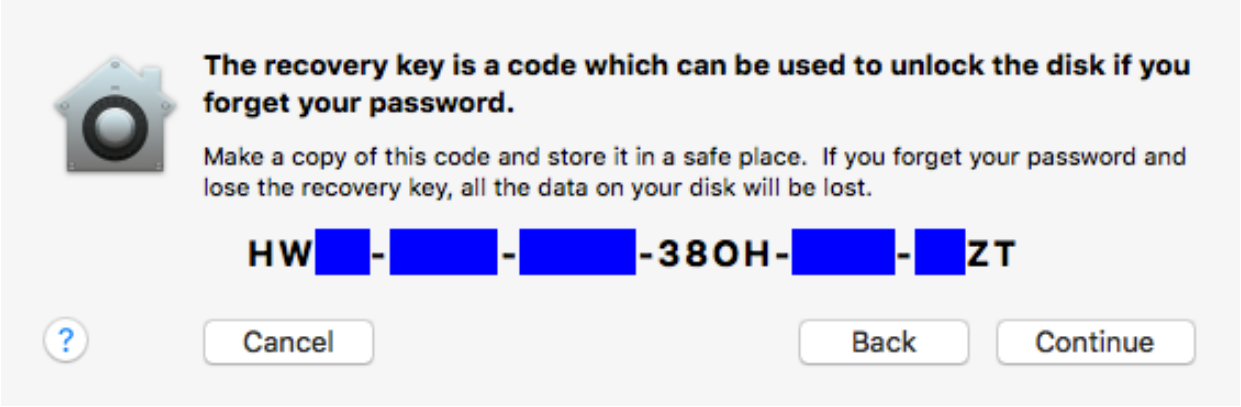
3.1 After clicking the **Turn On FileVault** button, you will be asked to restart your computer.



Follow the instructions in the message box and once your computer has restarted, return to Security and Privacy and click Turn On FileVault.

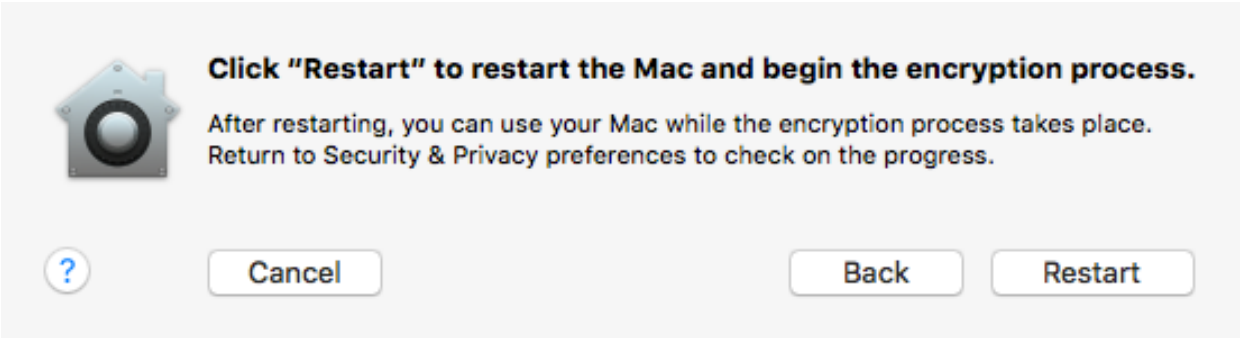
3.2 You now need to provide a location to store your recovery key, this can either be your iCloud account or your will be provided with the encryption key.

3.3 In this example, we will use a recovery key that is **not** stored in an iCloud account. So a twenty-four-character password is presented.



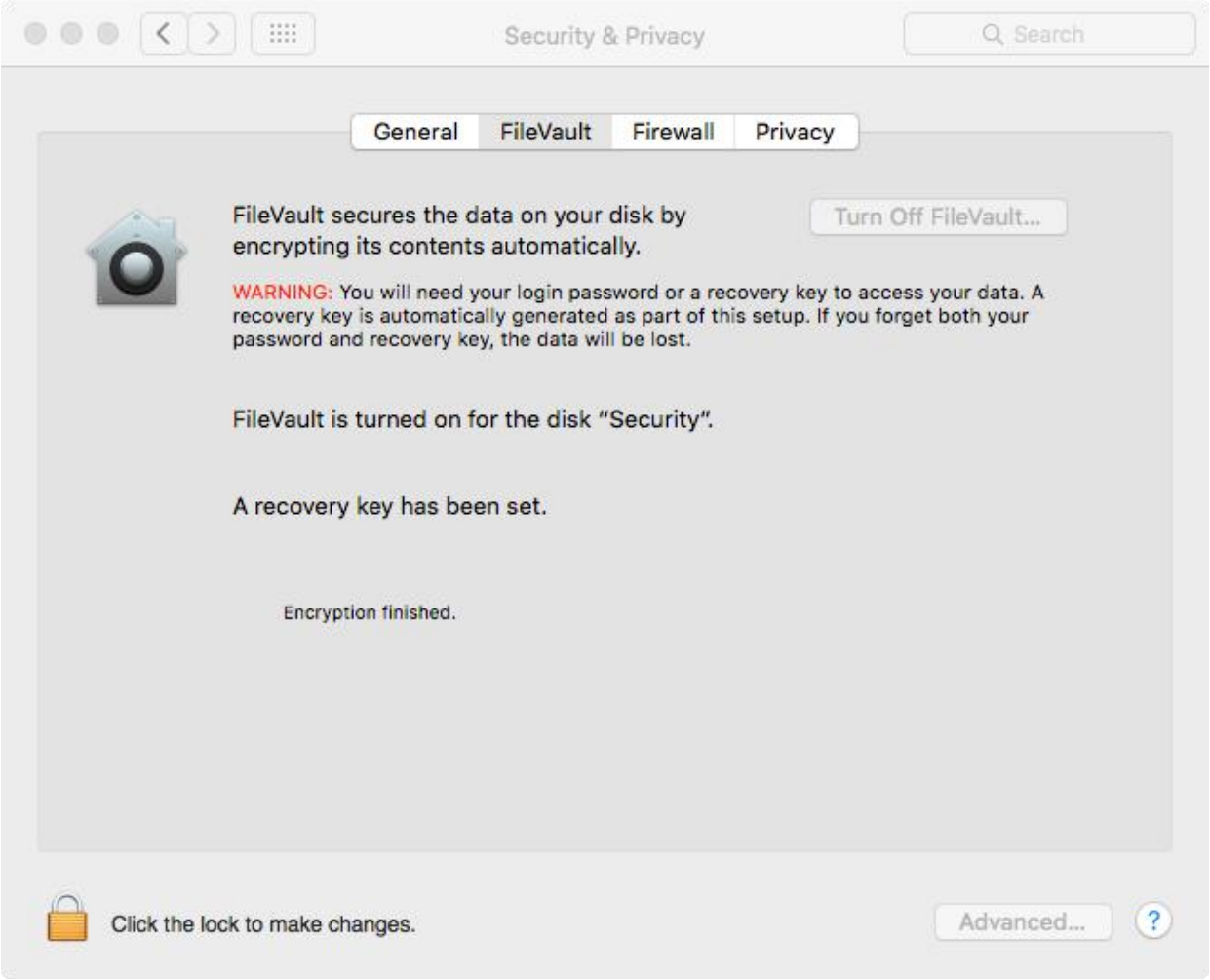
3.4 Please make sure that this key is kept securely, this key is required to decrypt the data on your computer. Without it you will not be able to access your information.

3.5 You are then required to reboot your computer once more; on this reboot the encryption process will start using the encryption key you have been provided with.



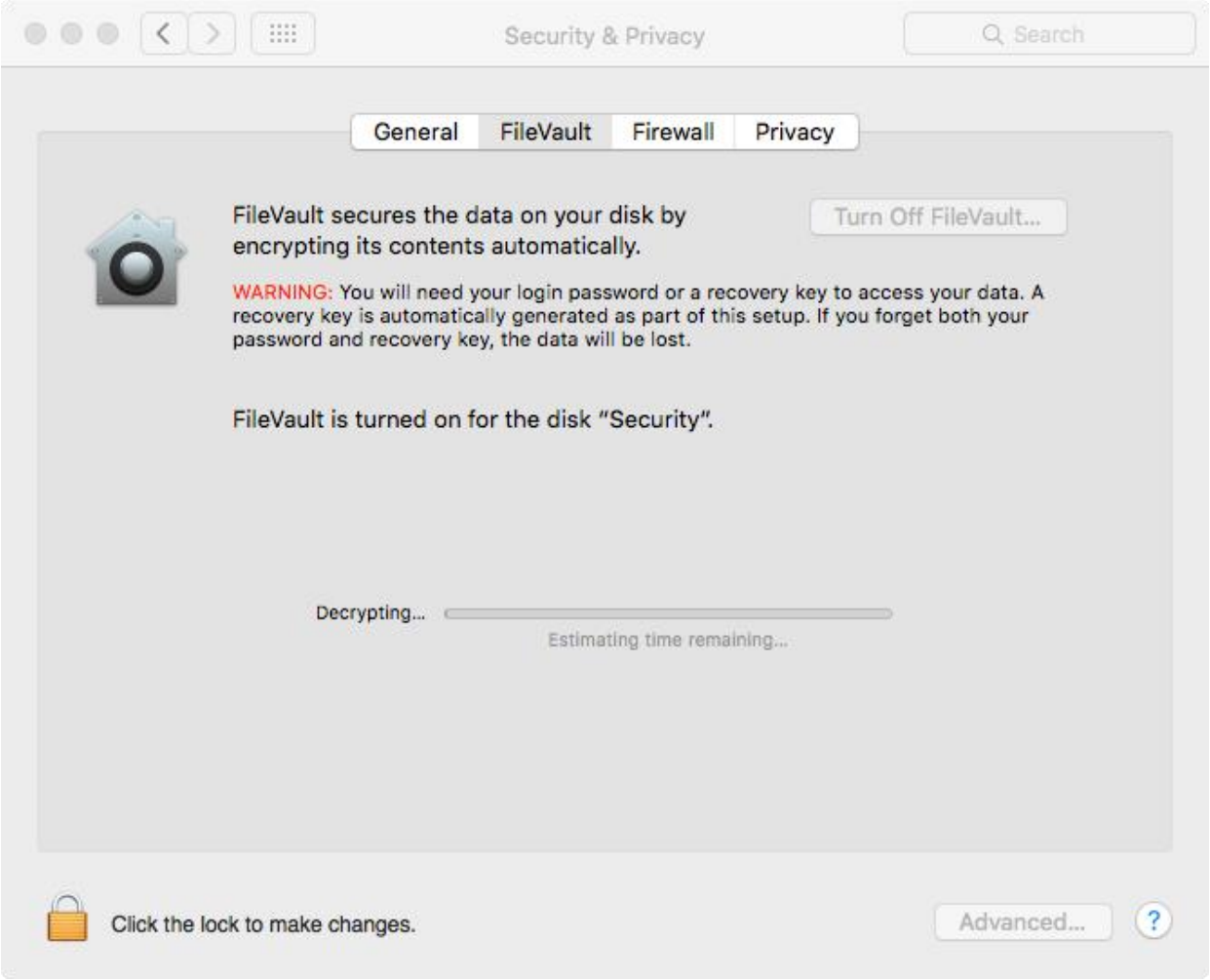
3.6 While your computer is encrypting, you are still able to perform your normal tasks on it, there should be little (if not no) impact on the performance of your computer during this time.

3.7 Upon completion of the encryption, you will see the Security and Privacy, FileVault is turned on for this device, a recovery key has been set and Encryption finished. The button that you pressed to Turn on FileVault will now let you decrypt your hard drive if required.



4. Decrypting a drive

4.1 In System Preferences go to Security and Privacy and from there select the FileVault tab, provide the username and password to allow changes (if required) and then click **Turn Off FileVault**. You will still be able to use your computing during the decryption process.



4.2 Once the decryption is complete, then the hard drive is no longer encrypted. **Please note** this means that the information on your device is only as secure as the device itself. If you lose the device anyone can access your personal data that is stored on it.