Encrypting Your Personally Owned Computer with FileVault

The University only requires Full disk encryption on your **personally owned computer** if you store confidential (Category I) or controlled (Category II) University data on it. You are not required to encrypt your personally owned computer if you do not store University data on it, always use a VPN to connect to an on campus computer to work, or only access data through web applications such as MyMav. The following instructions are provided to help you encrypt your personally owned computer using native filevault2 encryption. Before you proceed please make sure you have read all the notes and cautions:

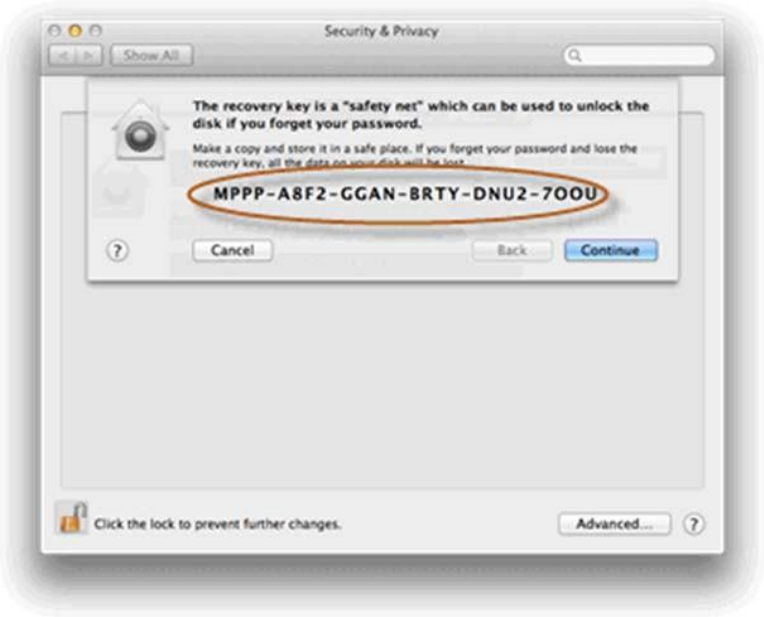
NOTES

- Filevault2 encryption is an Apple product and there are widely available instructions on the internet on how to encrypt your computer using it. The instructions provided are a best effort to simplify the instructions for you. They are provided "as is" and we do not make any warranties about its accuracy; you do not have to follow these instructions.
- Filevault2 does not work on all versions of Macintosh OS and there are alternatives to Filevault2 for full disk encryption.
- By opting to deploy full disk encryption on your personally owned computer, you are assuming all risks, including data loss. Before beginning the encryption process, make a backup of your data!
- All University owned computers are required to be encrypted using University approved encryption management software. **Do not use these instructions for University owned computers**. For more information on Approved software for University owned devices see https://www.uta.edu/security/encryption/fulldiskencryption/maintain_compliance.php
- You must safeguard your encryption key and keep it in a secure location.
- You may be required to provide this key to the University and make your personal computer available for e-discovery searches for University data in the event of open records requests, litigation holds or subpoenas.

Enabling FileVault for Your Mac:

1. Open ***System Preferences***.
2. Select the ***Privacy and Security*** icon.
3. In the next window, choose the ***FileVault*** tab.

4. Click ***Turn On FileVault***. OS X will generate a recovery key. Store this key in a safe and secure place:



5. Apple requests that you share this key with them. However, this is ***against*** UT Arlington policy.

6. Finally, you will be prompted to restart in order to begin the encryption process.

In order to check the status of the encryption process, you can open the ***FileVault*** screen.