Encrypting Your Personally Owned Computer with BitLocker

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 BitLocker encryption. Before you proceed please make sure you have read all the notes and cautions:

NOTES

- BitLocker encryption is a Microsoft 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.
- BitLocker does not work on all versions of Microsoft Windows and there are alternatives to BitLocker 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.

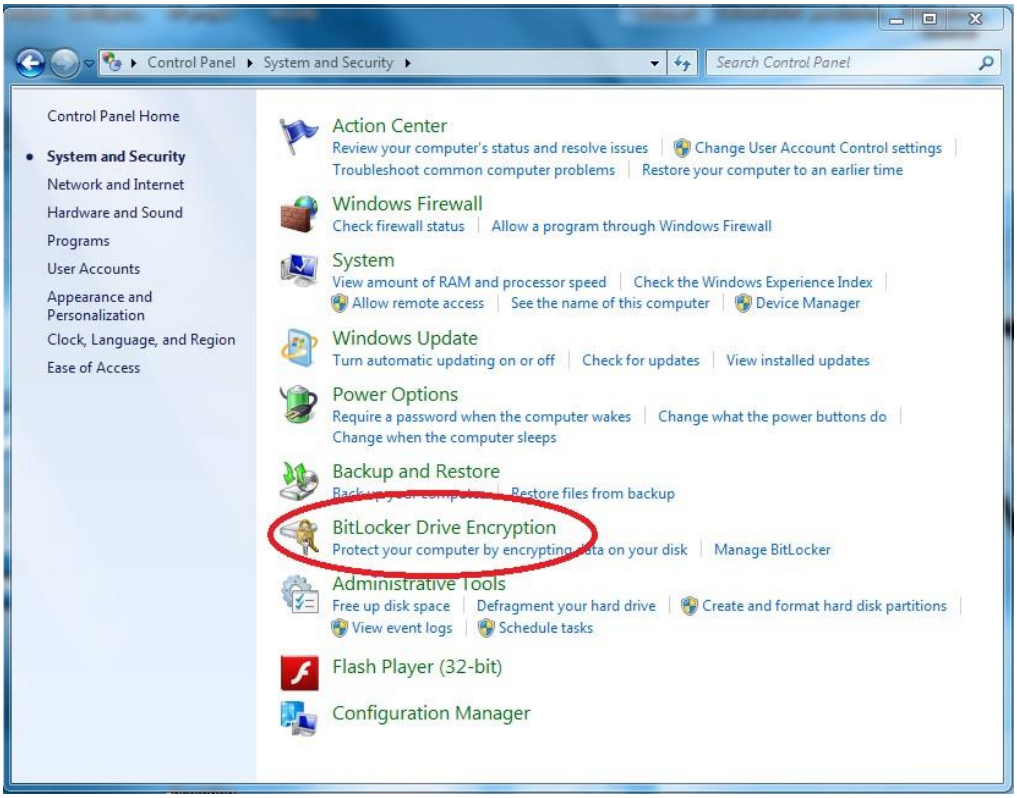
IMPORTANT NOTES:

Always Use disk validation tools to check for disk errors. Disk errors often indicate a drive is beginning to fail. The encryption process involves intensive writes to the hard disk, and can sometimes accelerate a failure. On Windows operating systems, run chkdsk.exe to check for errors.

- Close all open programs and files before you begin the encryption process.
- Verify that your computer is running Windows 7 **Ultimate** edition or higher (other versions do not have BitLocker).
- Verify that TPM is enabled in your computer's BIOS. If your computer does not have the TPM chip, you can use a dedicated USB flash drive to enable BitLocker. *(Instructions for devices without the TPM chip are at the end of this document.)*

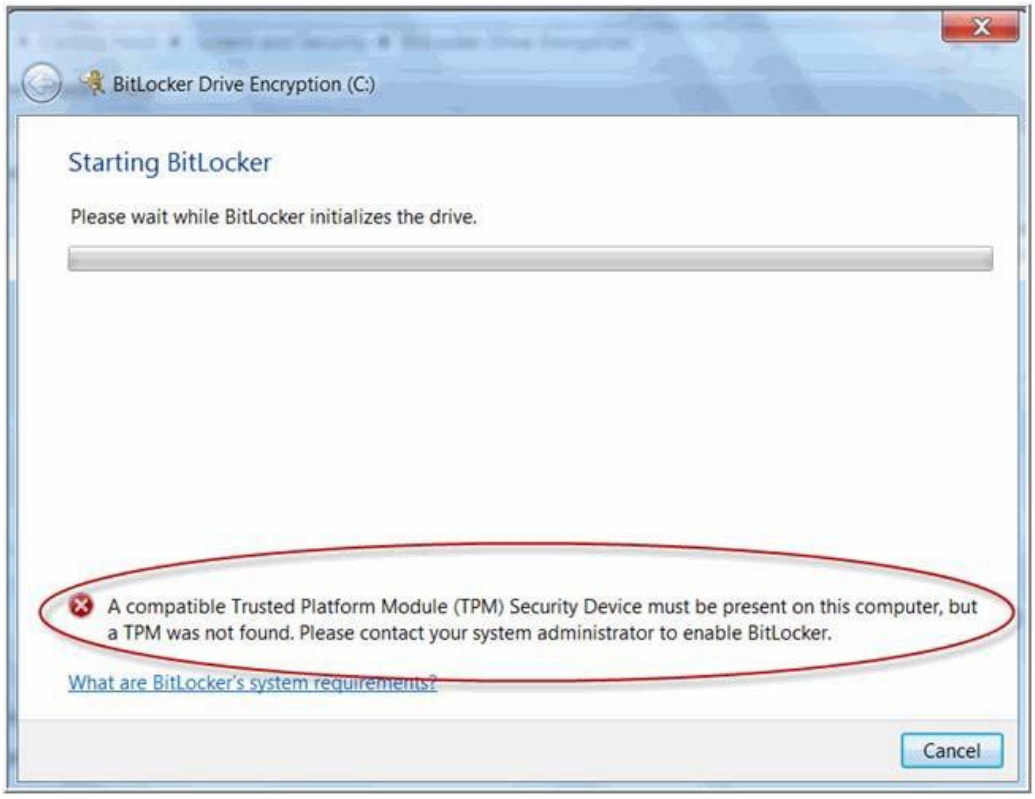
Enabling BitLocker:

- Open the ***Control Panel.***
- Click on ***System and Security.***
- Click on ***BitLocker Drive Encryption***.



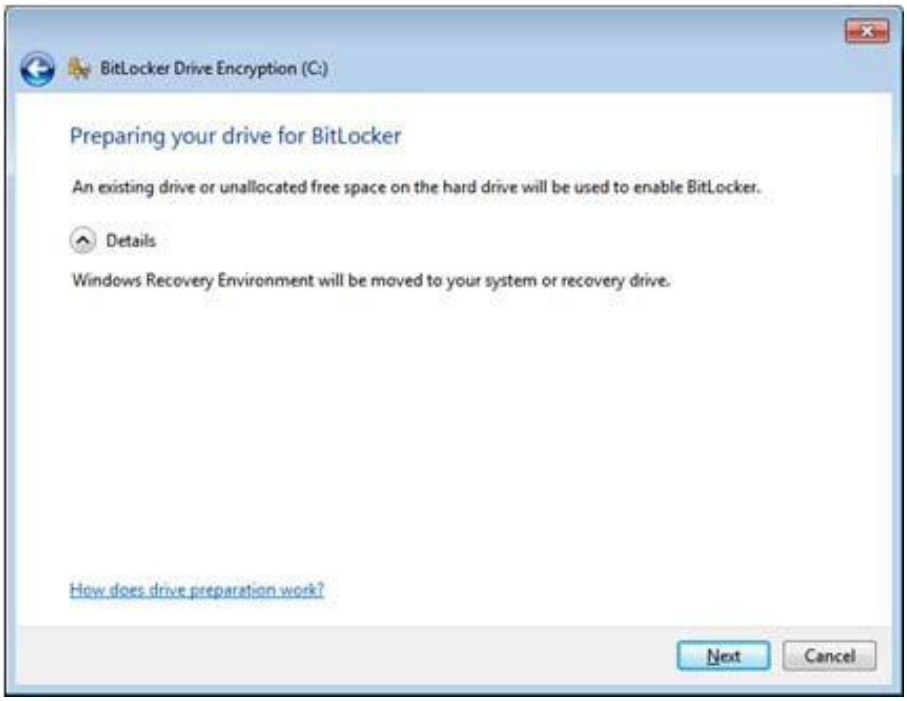
1. Click ***Turn on BitLocker.***

2. If you see a message similar to the one below, you will need to use the Non-TPM device instructions at the end of this document.

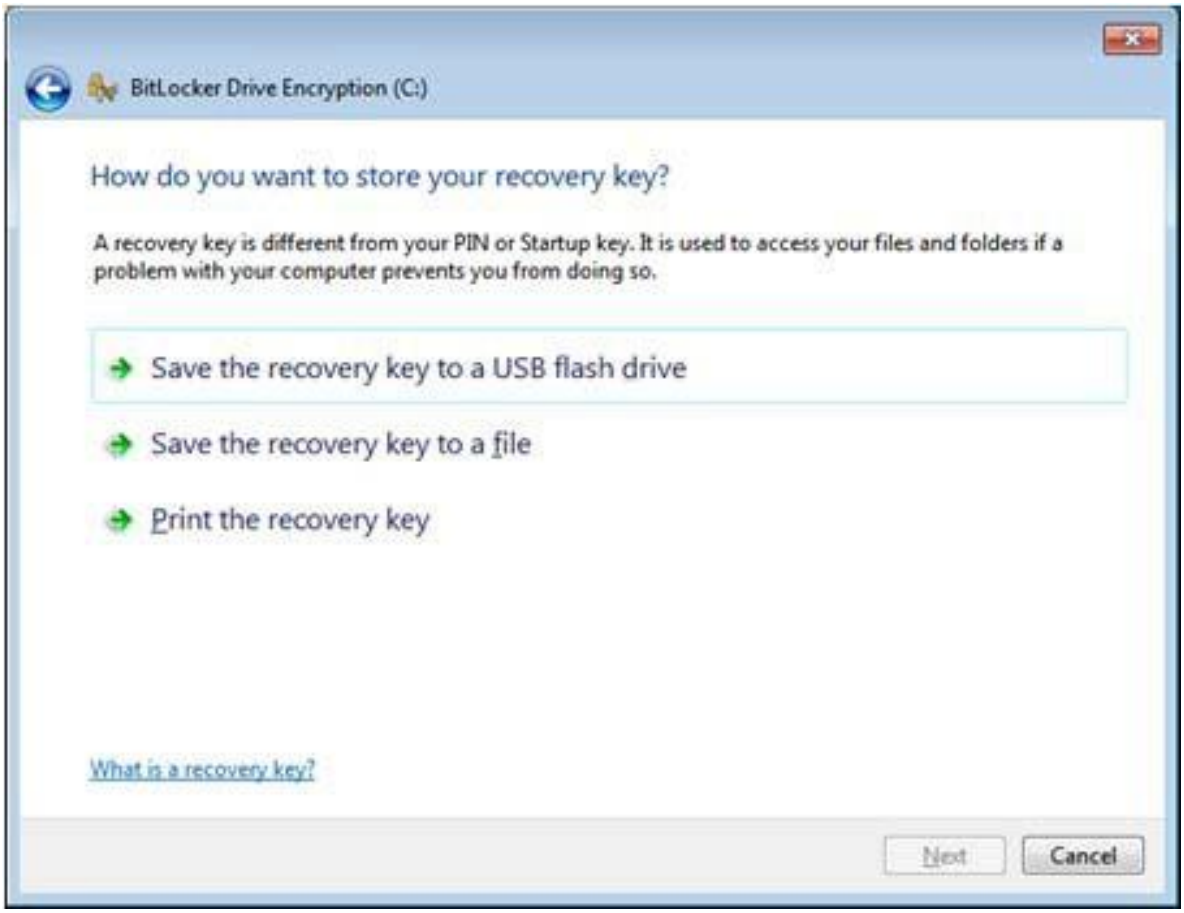


3. Otherwise, Windows will analyze what needs to be done. Click ***Next***.

4. Click ***Next***.



5. In order to enable TPM, the computer may reboot and require that you grant permission. Follow your computer's specific instructions.
6. When Windows begins to encrypt the drive, you'll be prompted for how to save the recovery key. You may not save the key to an encrypted drive. Select the option that you prefer, but remember to save the key in a safe place and secure place.



7. Once the key has been saved, Windows will prompt you to run a system check. This is recommended. Click ***Continue*** to start the system check.

After your computer reboots, windows will begin the encryption process. You can check on the status by going to ***Control Panel -> System and Security -> BitLocker***

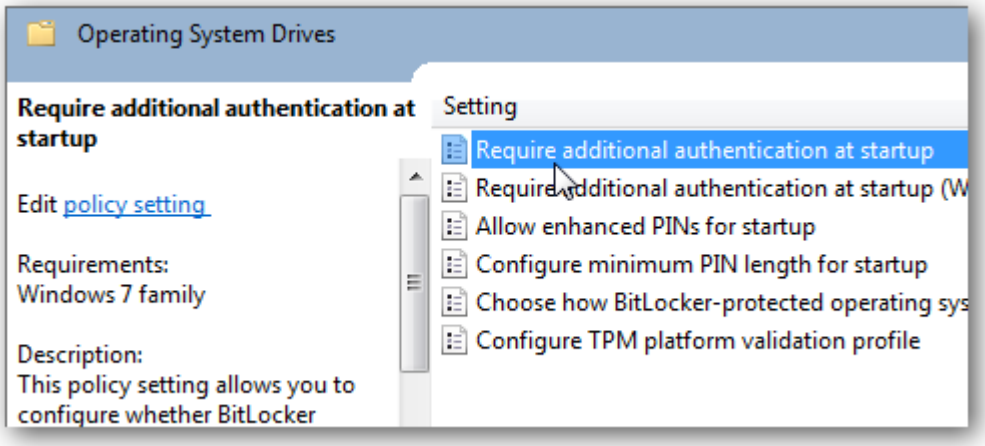
Non-TPM device instructions

TPM stands for “Trusted Platform Module” which is a microchip in a computer that supports advanced security features. It’s where BitLocker stores the encryption key. If you have a drive that doesn’t have a compatible TMP then you’ll need to use the following steps and have a dedicated flash drive ready. You will need this flash drive every time you start the computer.

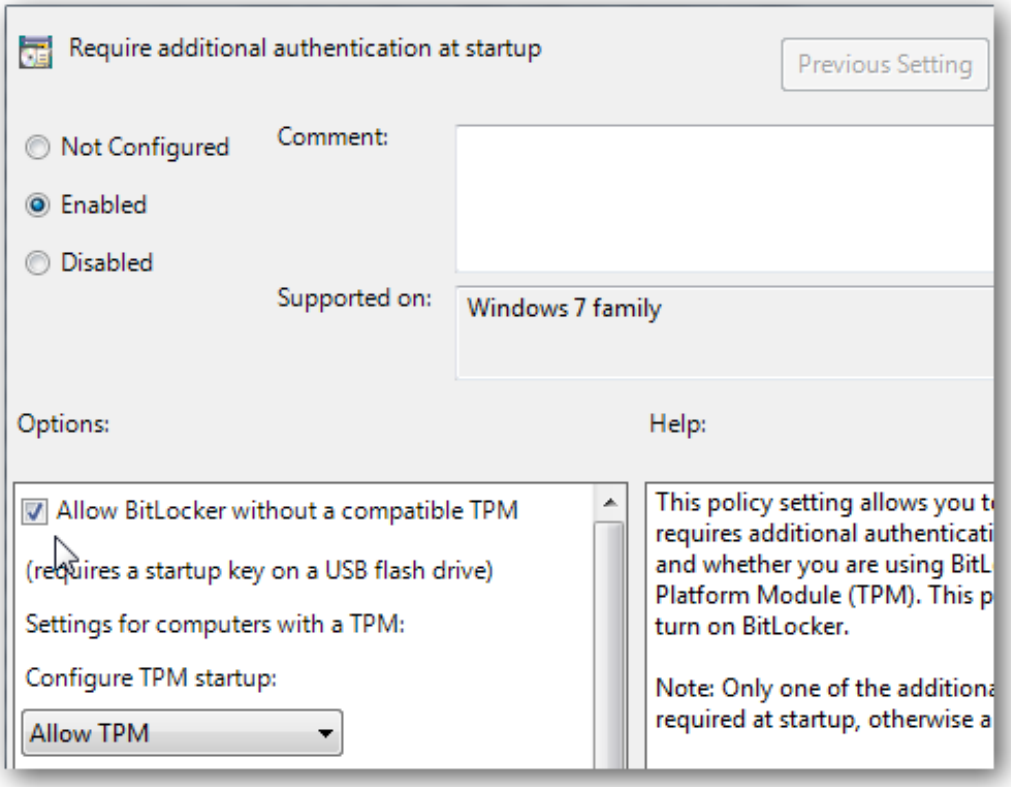
NOTE: you will need to safeguard this flash drive. If you lose this drive you will not be able to access your computer.

1. Enter “gpedit.msc” in the search box of the Start menu and hit Enter.

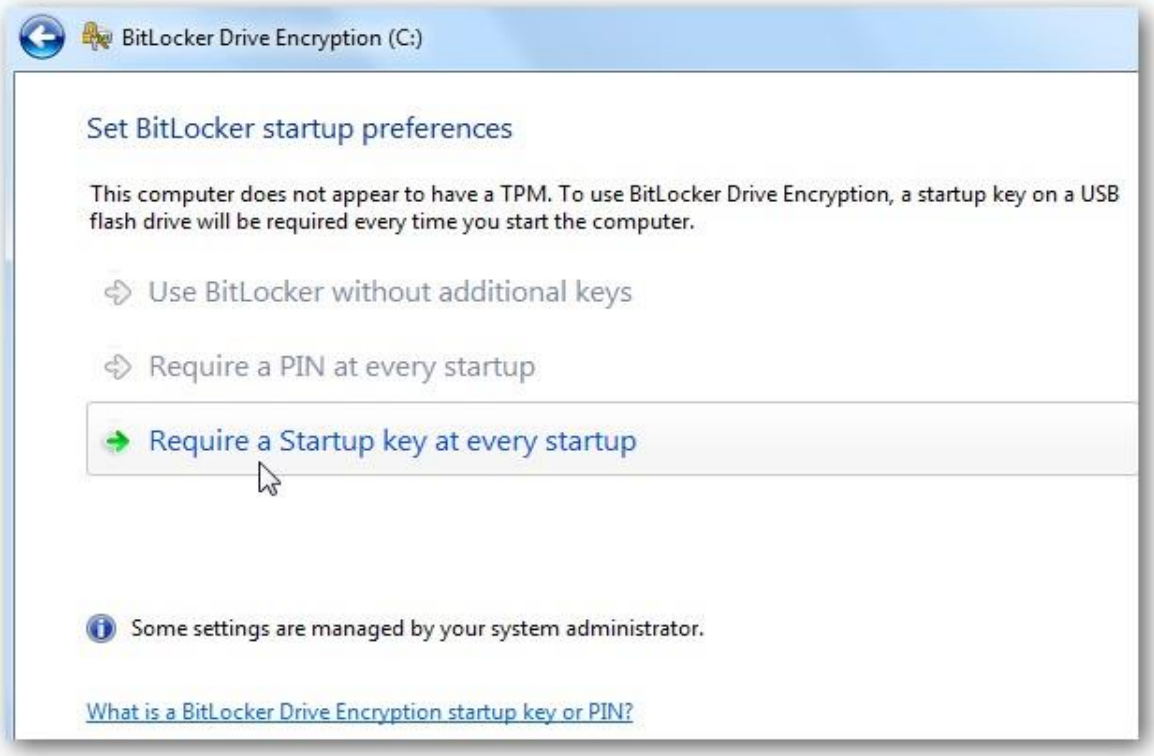
2. Under Local Computer Policy navigate to Computer Configuration \ Administrative Templates \ Windows Components \ Bit Locker Drive Encryption \ Operating System Drives and double click on Require additional authentication at startup.



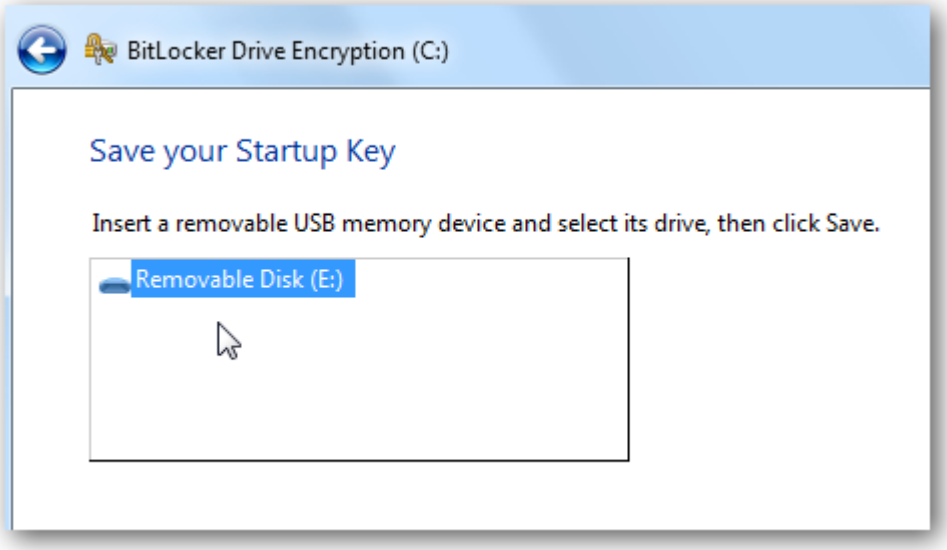
3. Enable the feature and check the box next to Allow BitLocker without a compatible TPM, click Apply and Ok, and close out of Local Group Policy Editor.



4. Go back to the hard drive you want to encrypt and turn on BitLocker. A restart will be required to prepare the disk, and at this point make sure the flash drive is plugged in. After the restart you're prompted to use the startup key on the flash drive every time you start the computer.



5. Select the drive (which you have already plugged into an available USB port on your computer) that you want you use to store the key.



6. Continue the encryption as above.