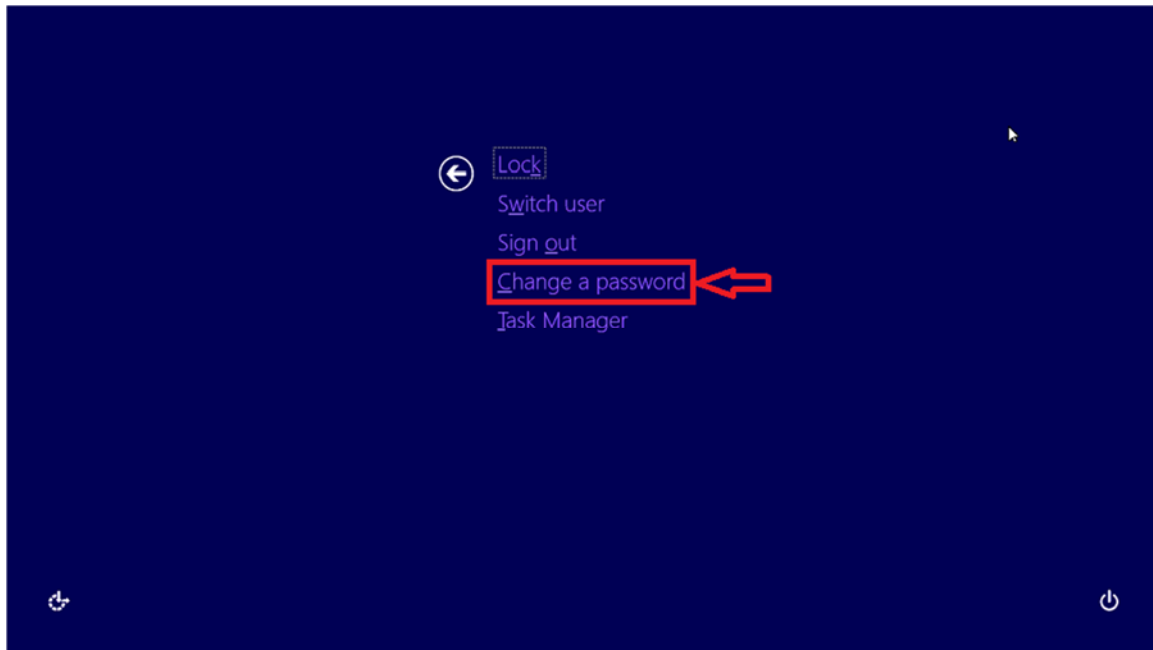


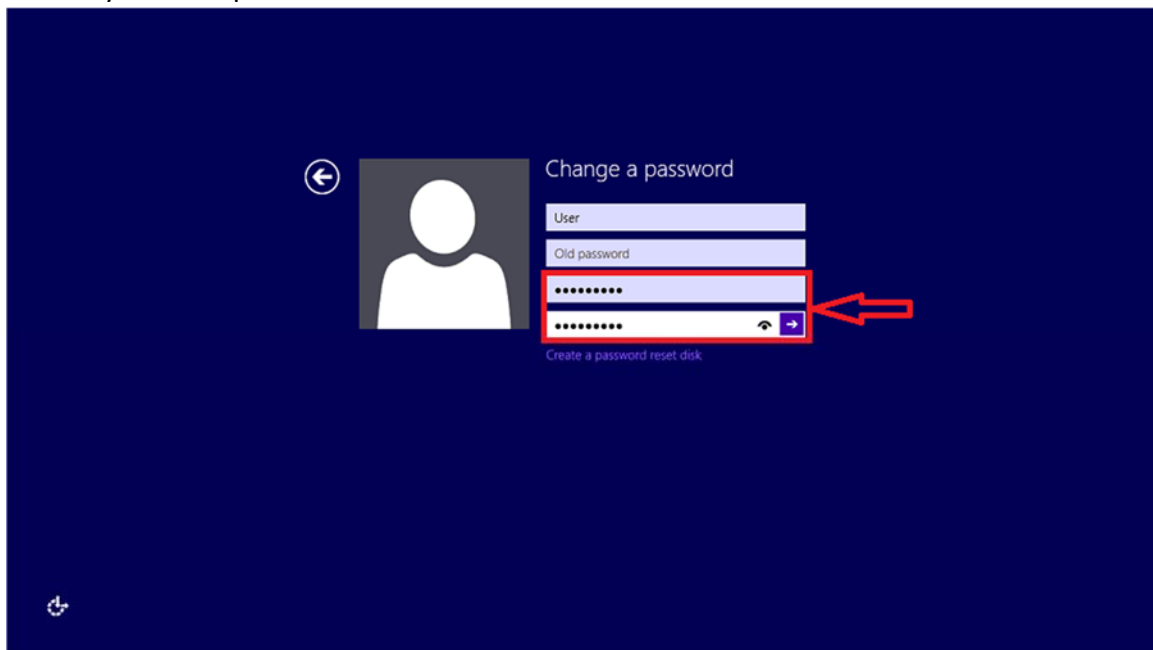
# BitLocker Encryption Guide

## 1. Create User Password (If you haven't already done so) :

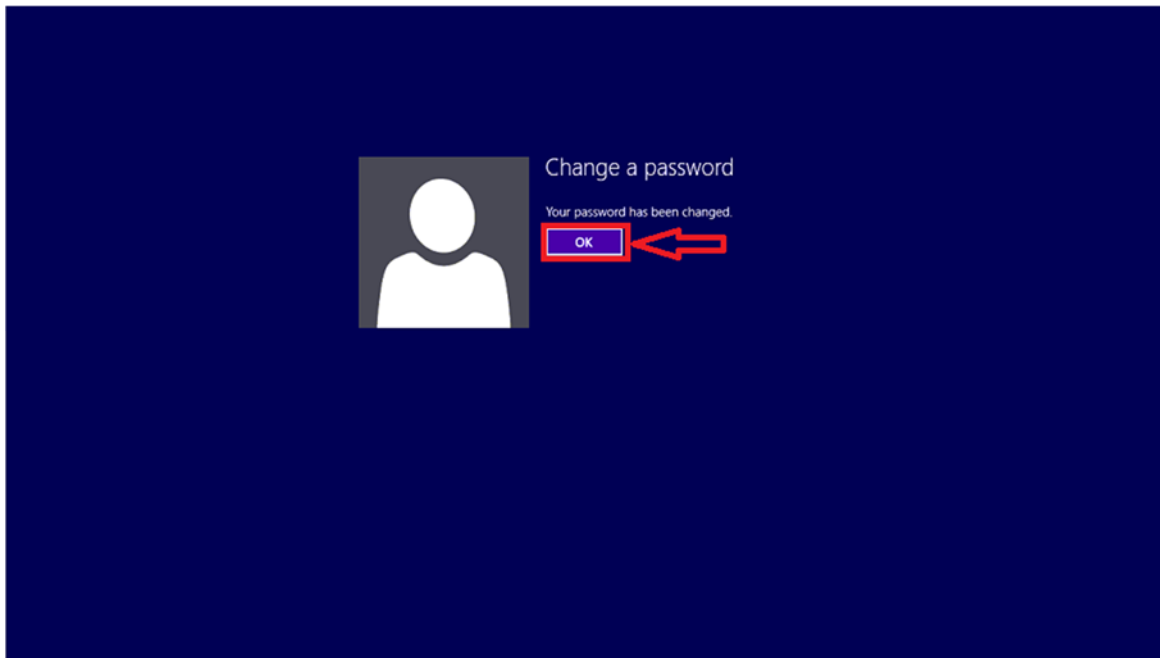
a. Press Ctrl+Alt+Delete, click **Change a password**.



b. Set your new password and confirm.

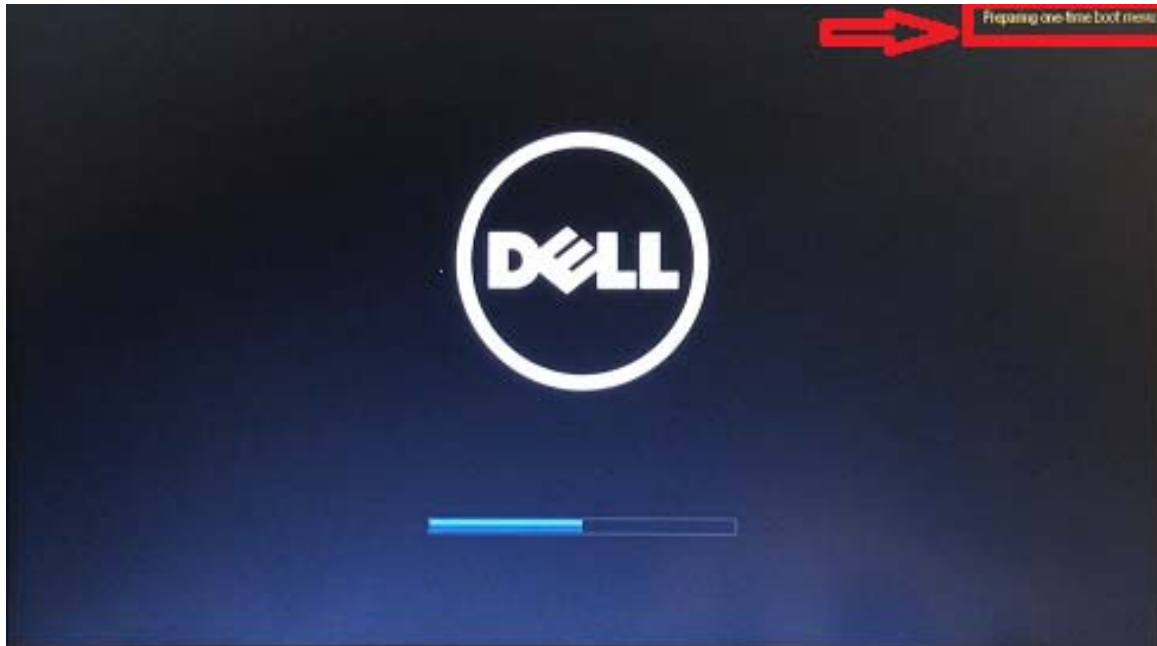


c. Click **OK**.

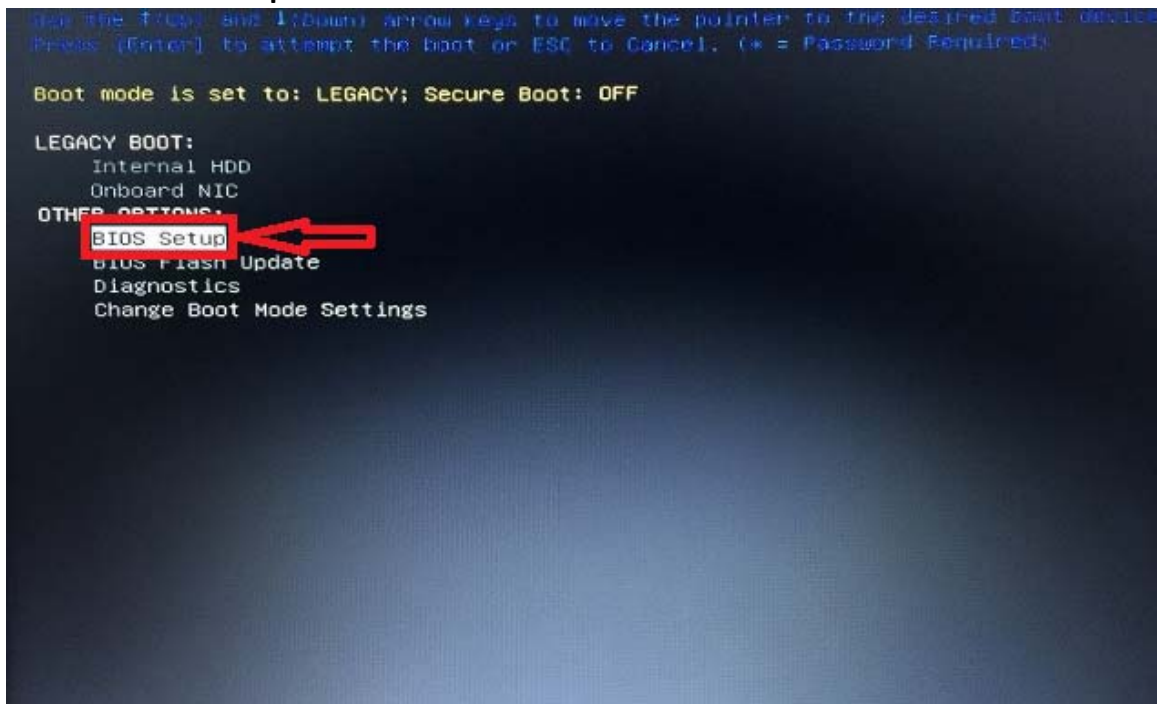


## 2. Activate TPM (Trust Platform Module) Chip:

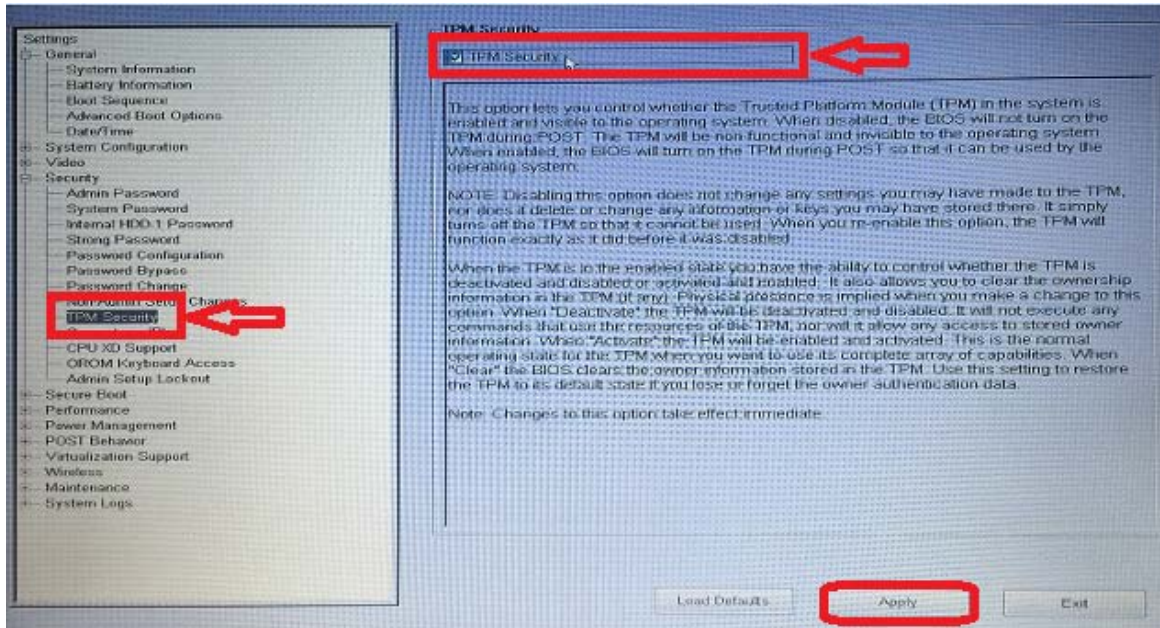
- a. After turning on the computer, repeatedly press **F12** after the Dell logo appears. A message, Preparing one-time boot menu..., will show on top right corner.



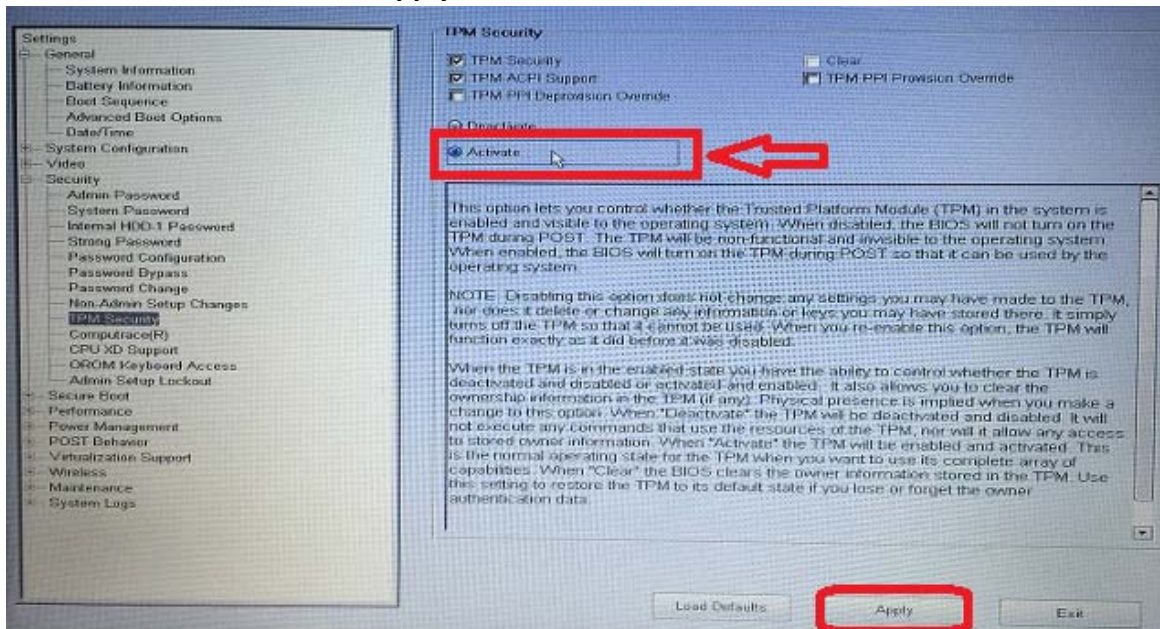
- b. Select **BIOS Setup**.



- c. On the left panel, go to **Security – TPM Security**.  
On the right panel, check **TPM Security** and click **Apply**.



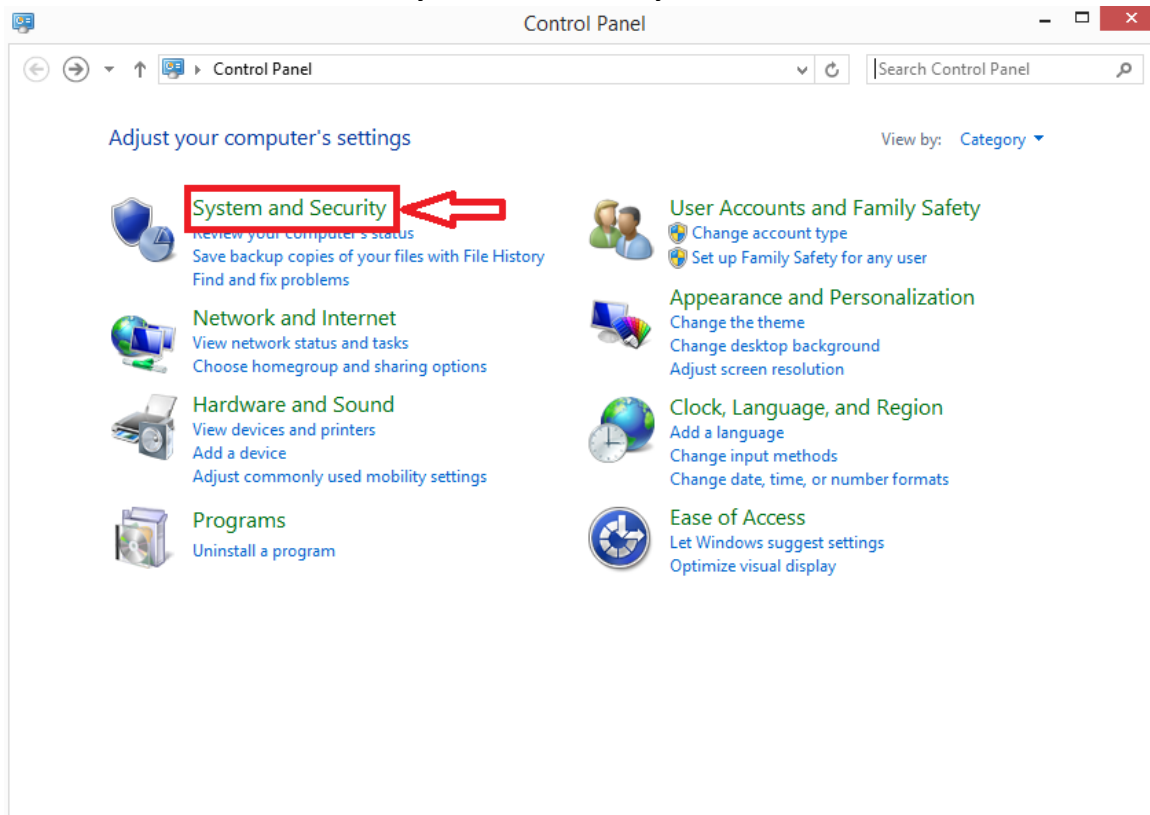
- d. Select **Activate** and click **Apply**.



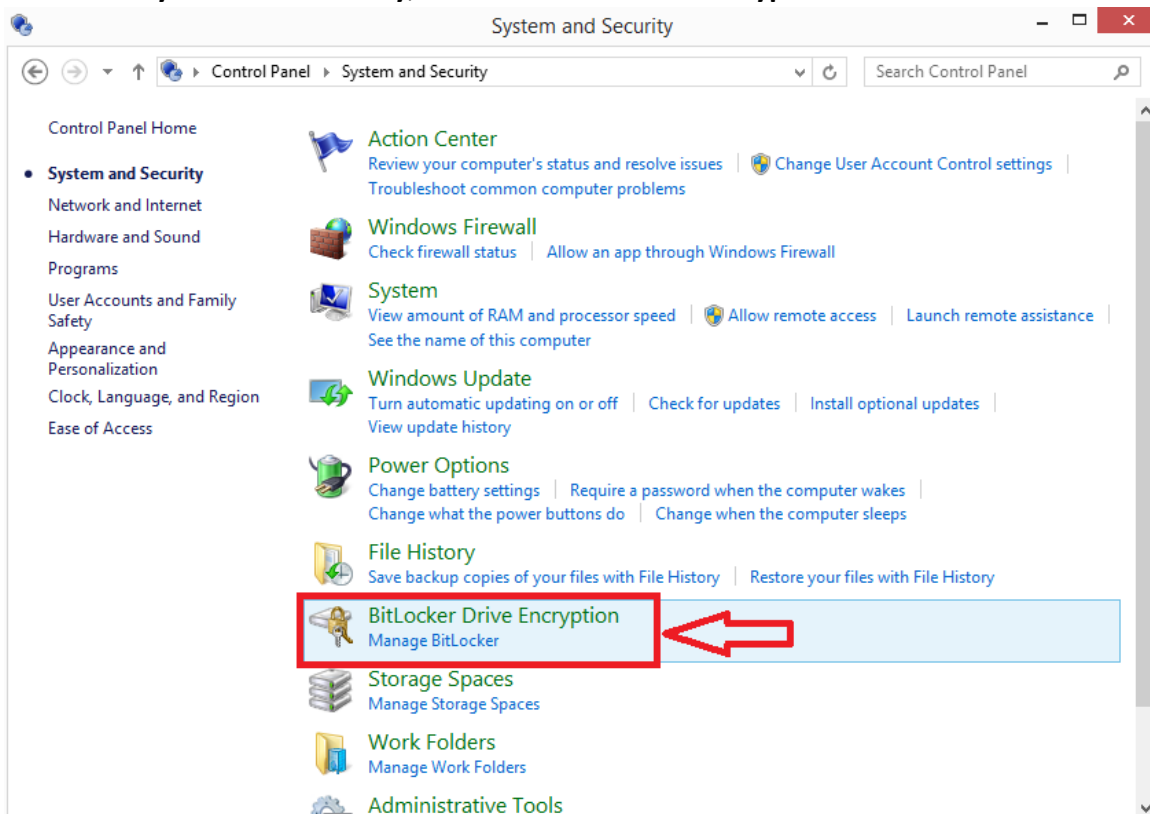
- e. **Exit** to restart the computer.

### 3. Enable BitLocker Encryption:

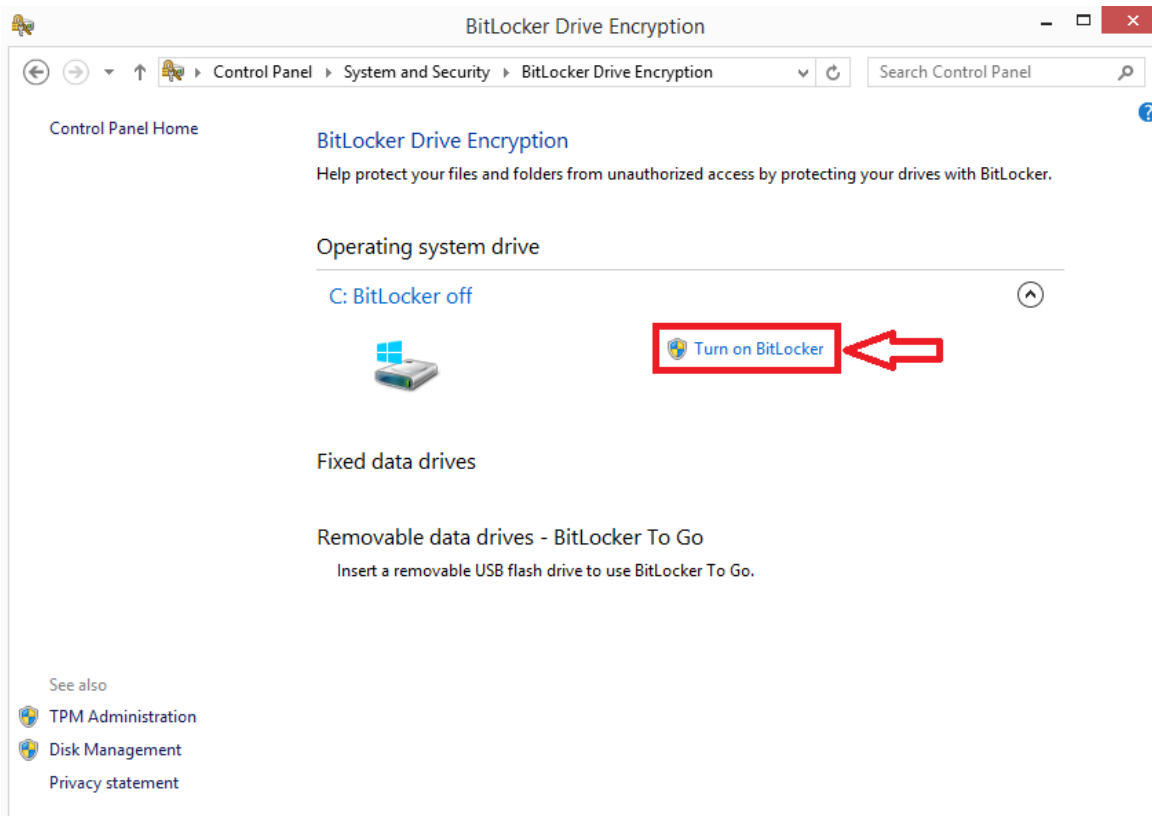
a. Under **Control Panel**, click **System and Security**.



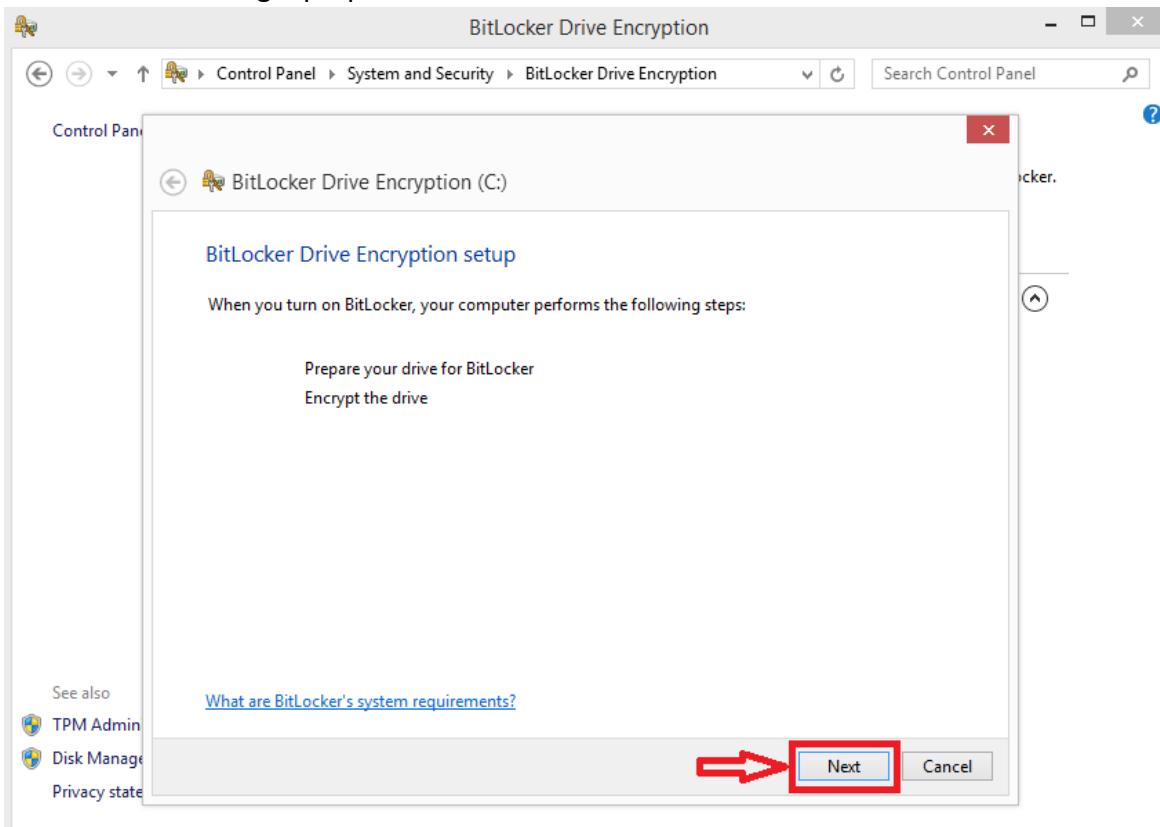
b. Under **System and Security**, click **BitLocker Drive Encryption**.



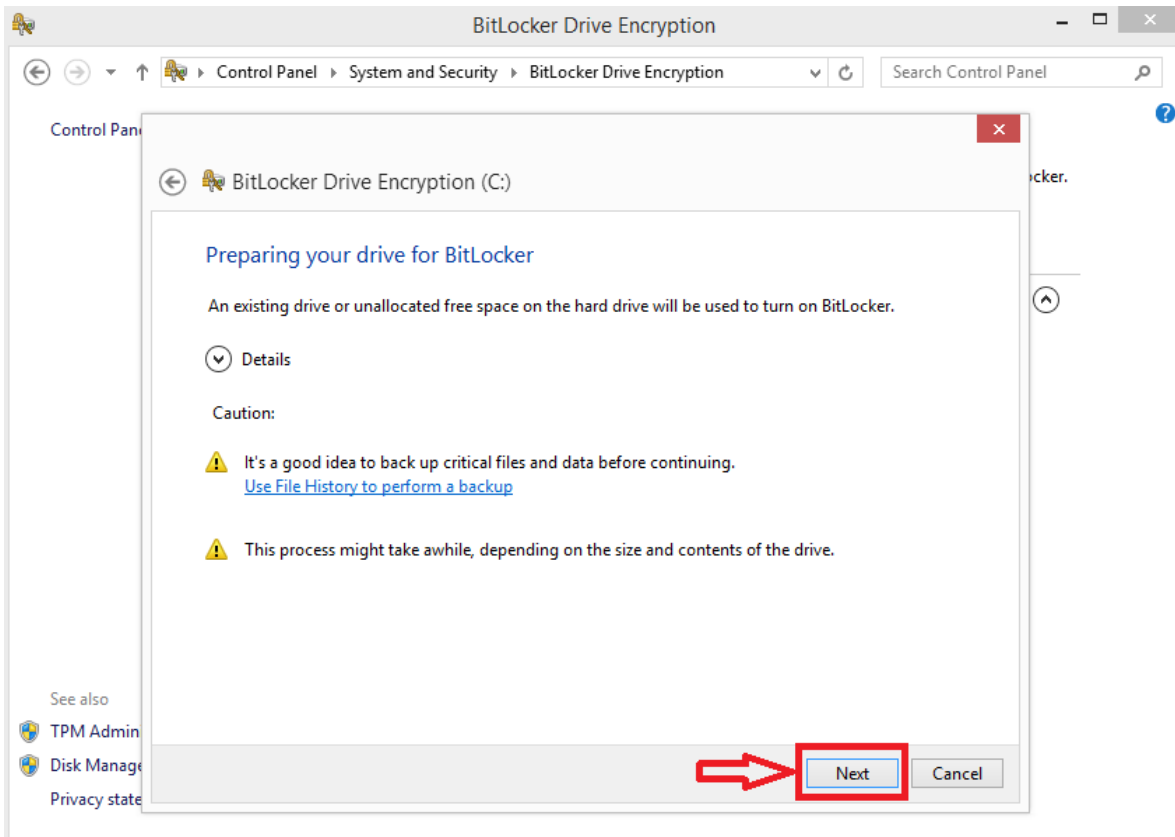
c. Click **Turn on BitLocker**.



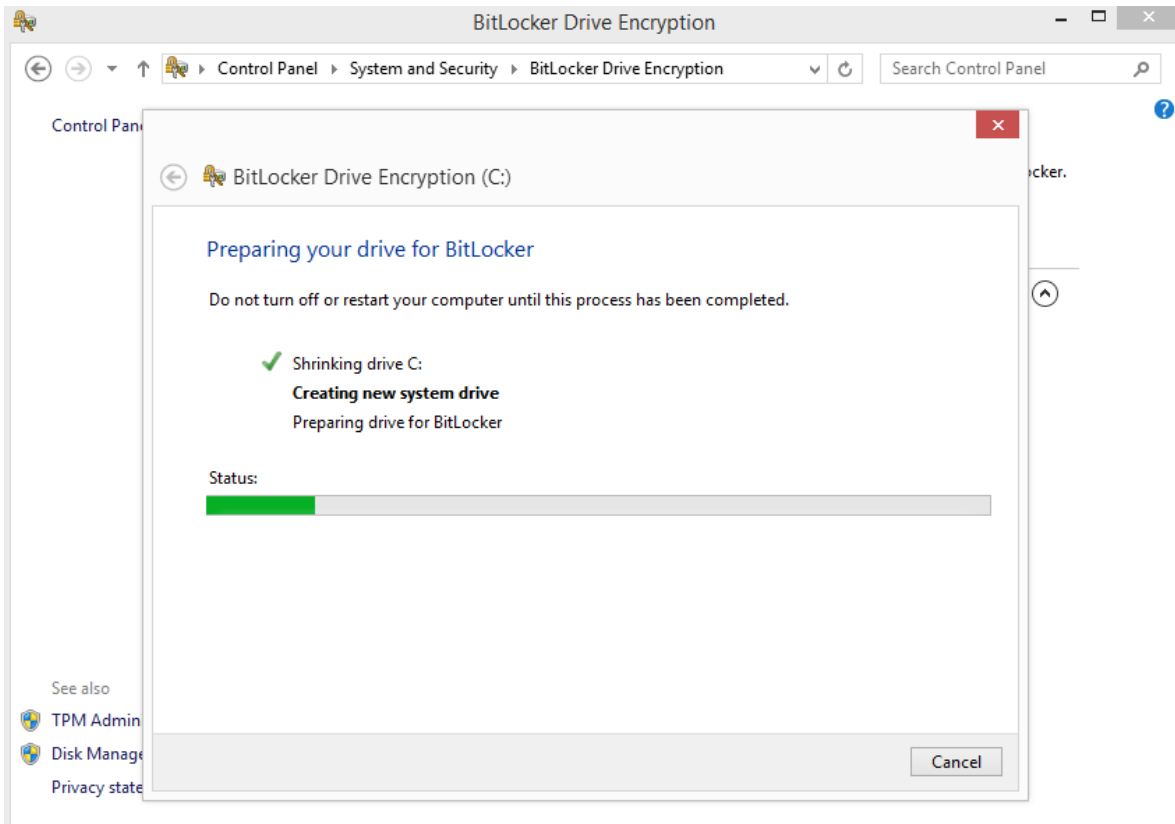
d. Click **Next** to begin prepare drive for BitLocker.



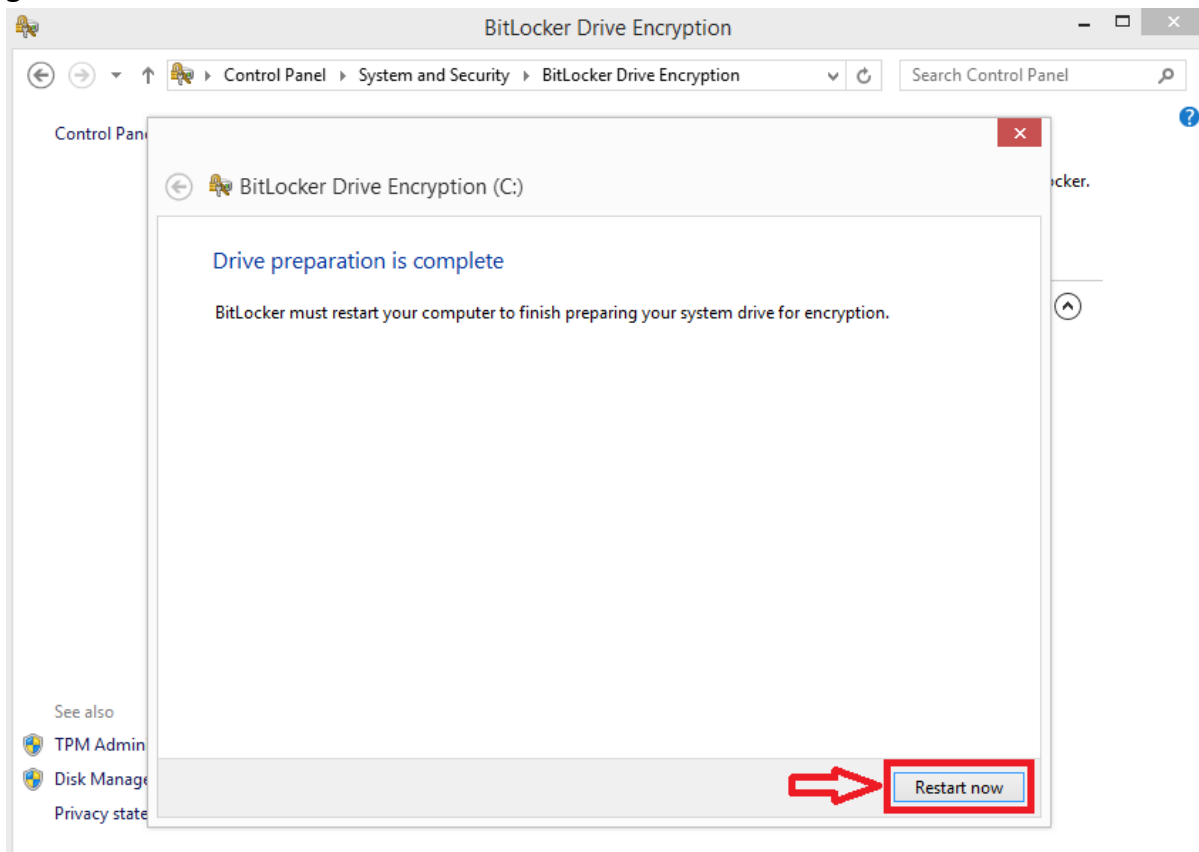
e. Backup personal data before encrypting the drive to prevent data loss, click **Next** to continue.



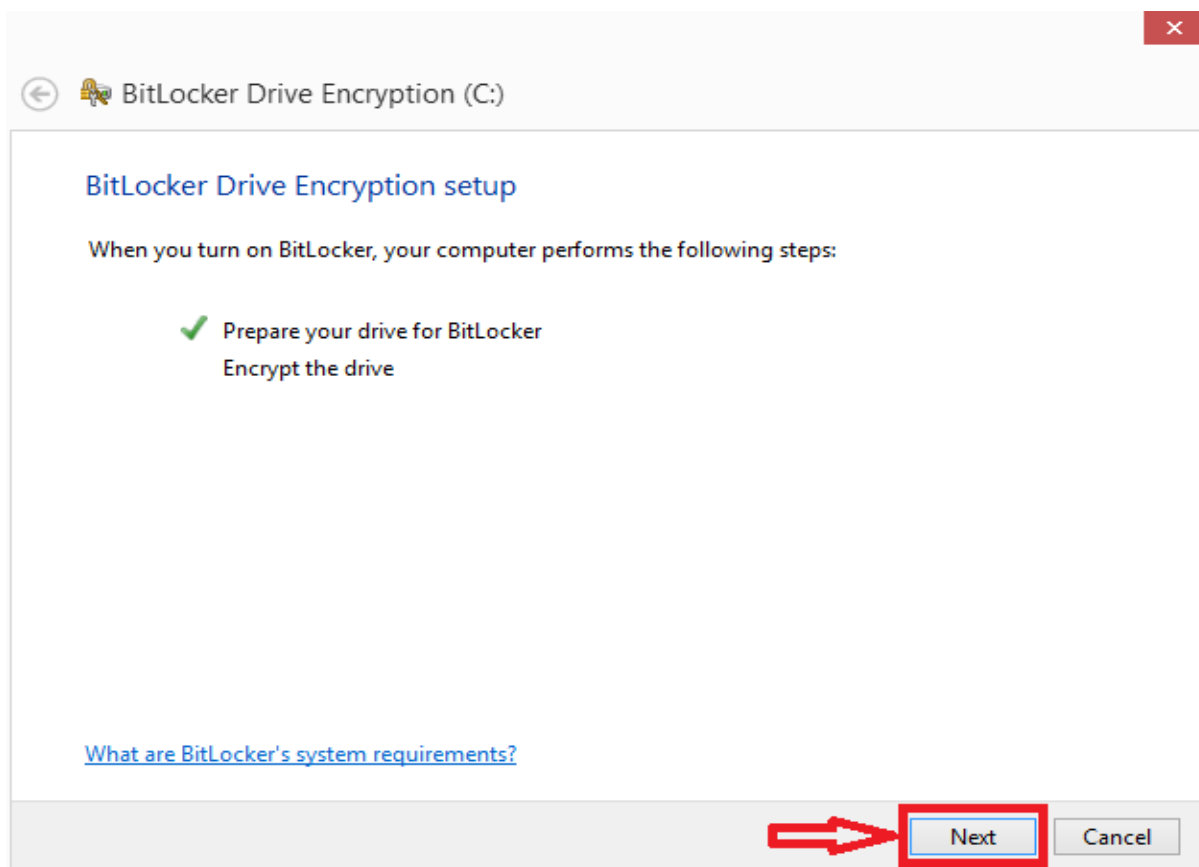
f. The preparing process should finish in few minutes.



g. Click **Restart now**.



h. After the computer restarts, BitLocker Drive Encryption will pop up automatically. Click **Next** to continue.

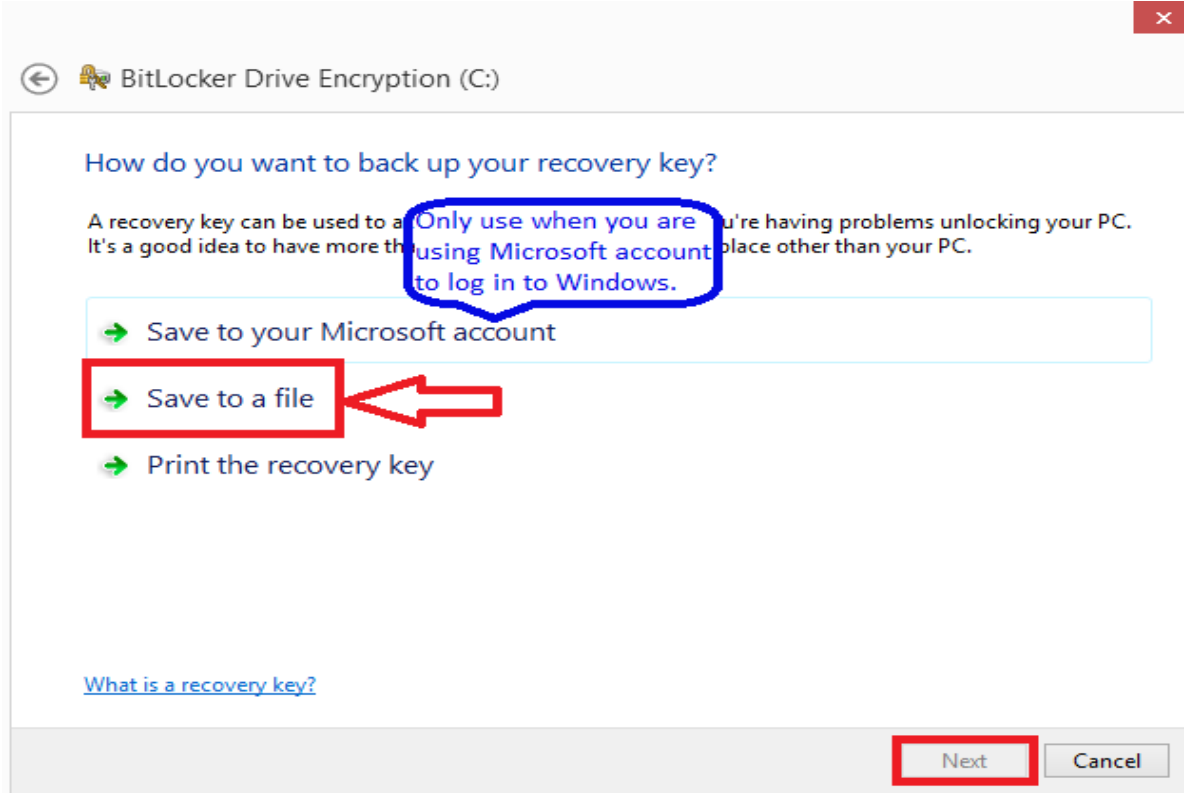




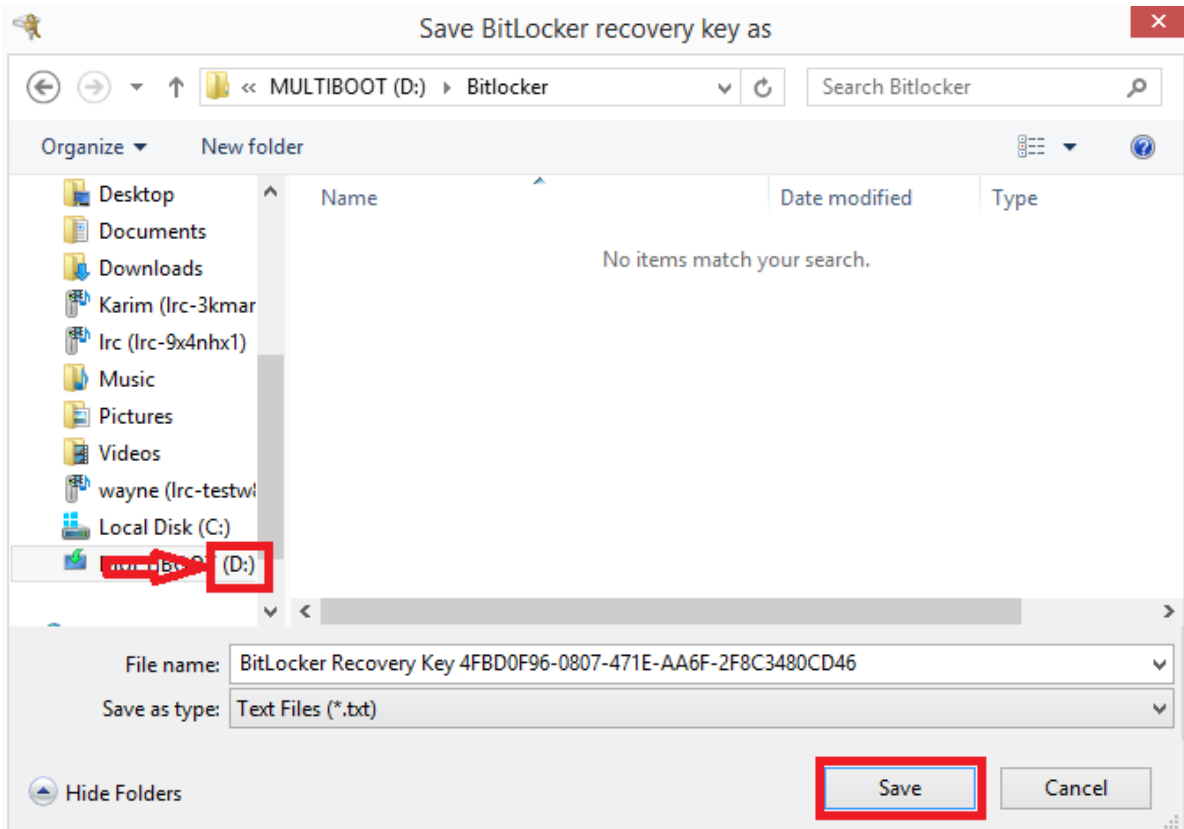
- i. You will need an external USB drive to save the recovery key. After you insert the USB drive, click **Save to a file** to continue.

If you login using your Microsoft account, you can save the key under your account.

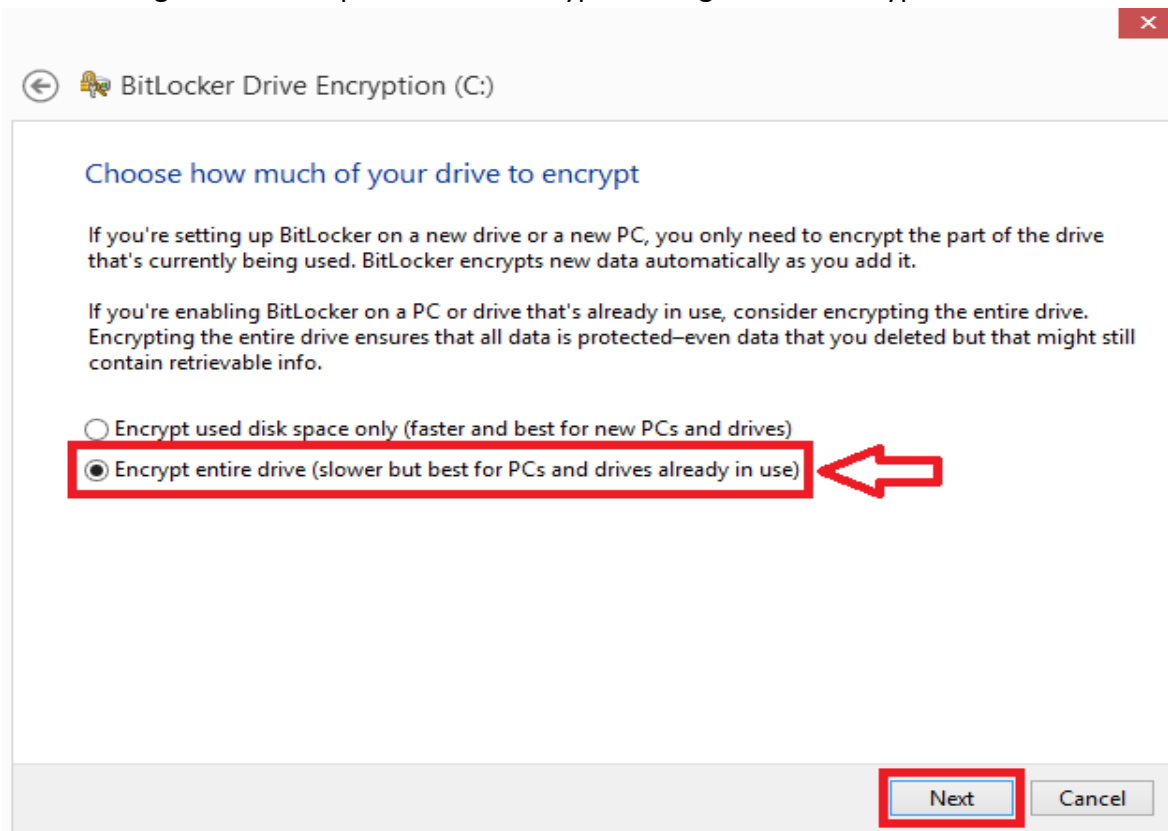
**Important:** Keep this key in a safe place and readily accessible to you if you need to use it.



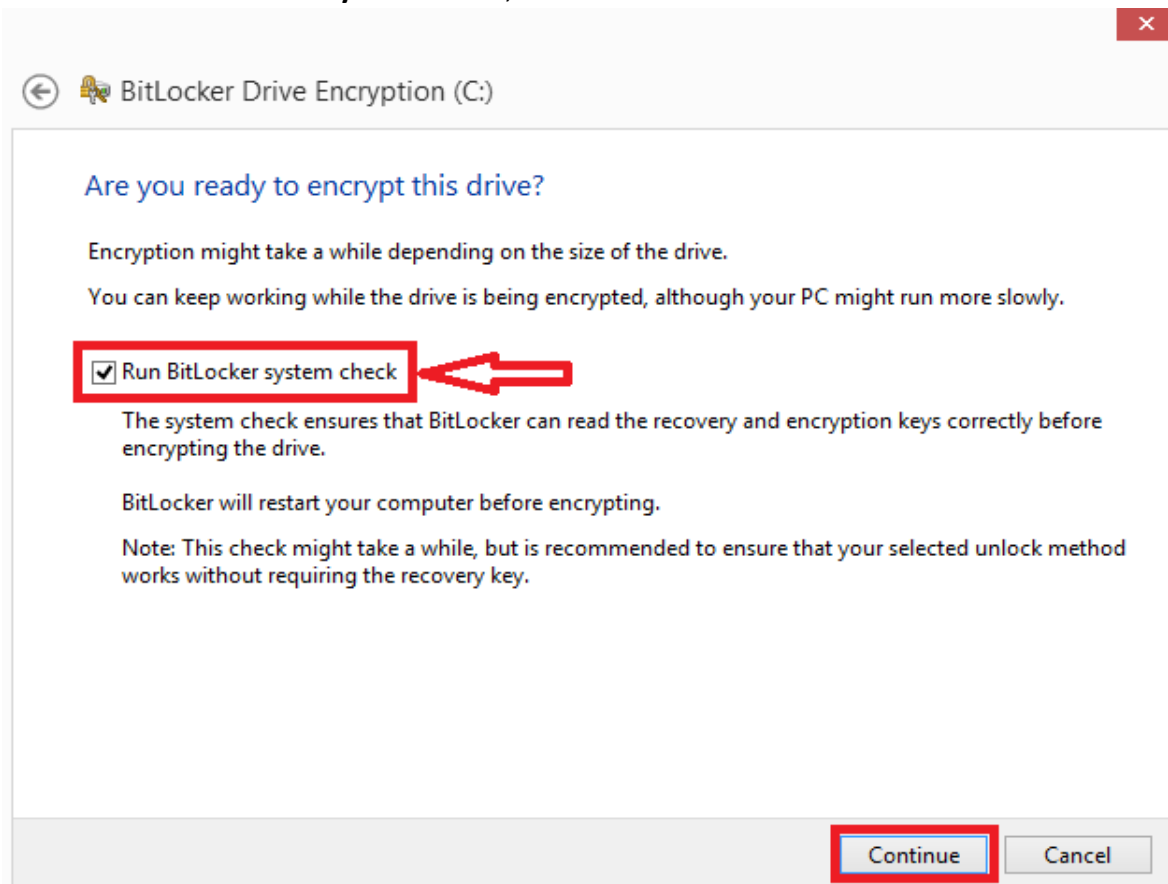
- j. Navigate to the designated drive, click **Save** to store the key.



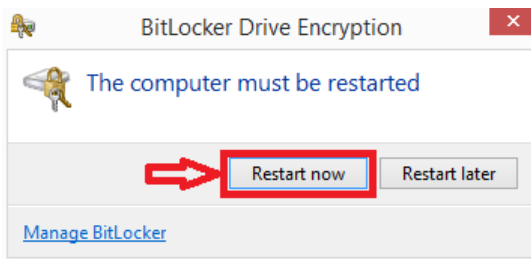
- k. Make sure to select **Encrypt entire drive** for full disk encryption. UTHealth MSIT policy requires all incoming student computers to be encrypted using full disk encryption. Click **Next** to continue.



- l. Check **Run BitLocker system Check**, click **Continue**.



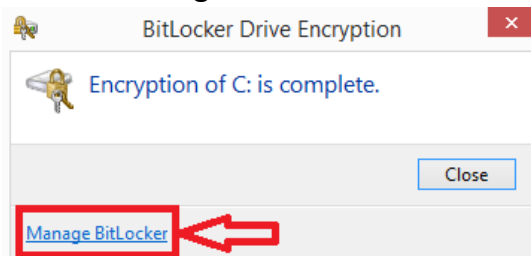
m. Click **Restart now**.



n. After the computer restarts, the encrypting process will begin. Normally, SSD Hard Drive will take less than 2 hours to encrypt depend on the size of the hard drive. You can still use the computer during the process.



o. Click **Manage BitLocker** to make sure the encryption is successful.



p. Your computer is now encrypted with BitLocker.

