BitLocker Encryption Guide

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

   a. Click the Search button (1) and type “Sign-in options” (2). Select Sign-in options (3).

   ![Search and Sign-in options screenshot](image)
b. Click “Change” to set your new password.
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. Click the Search button (1) and type “Control Panel” (2). Select Control Panel (3).

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

d. Click **Turn on BitLocker**.
e. Click **Next** to begin prepare drive for BitLocker.

![BitLocker Drive Encryption setup](image1)

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

![Preparing your drive for BitLocker](image2)
f. The preparing process should finish in few minutes.

![Preparing your drive for BitLocker](image1)

Click **Restart now**.

![Drive preparation is complete](image2)
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.
*Highly recommend, if you login using your Microsoft account, use first option (in **Blue**) to save the key under your Microsoft OneDrive account.

**Important:** Keep this key in a safe place and readily accessible when 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.
4. **Setting up 15 minutes inactive lock out:**

   a. Click the Search button (1) and type “Lock screen settings” (2). Select **Lock screen settings** (3).
b. Click Lock Screen. On the right side, click Screen Saver Setting.
c. Change the Wait time to **15 minutes** and check the box for **On resume, display logon screen**. Click **OK** to finish.