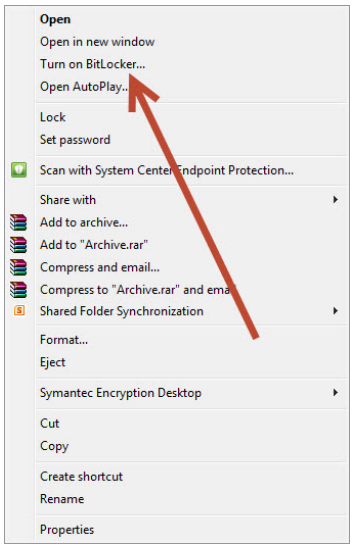
Guide to Encrypting USB and External Hard Drives in Windows

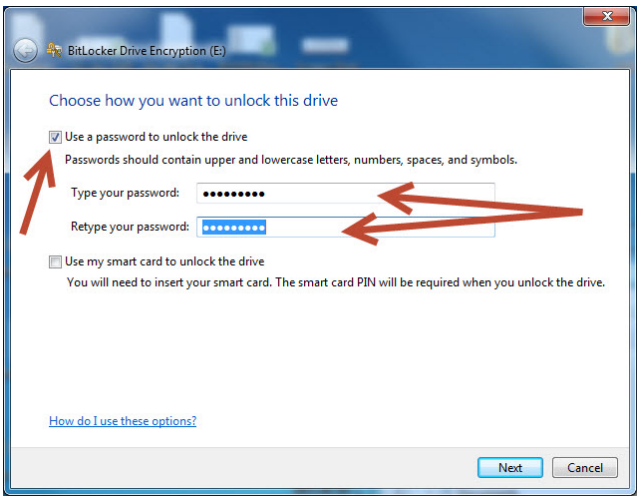
Purpose: This guide is meant to assist in encrypting a USB flash drive using Windows Bitlocker to Go.

It is important to back up any data you currently have on the USB before following the encryption steps below as the encryption process may cause data loss or corruption.

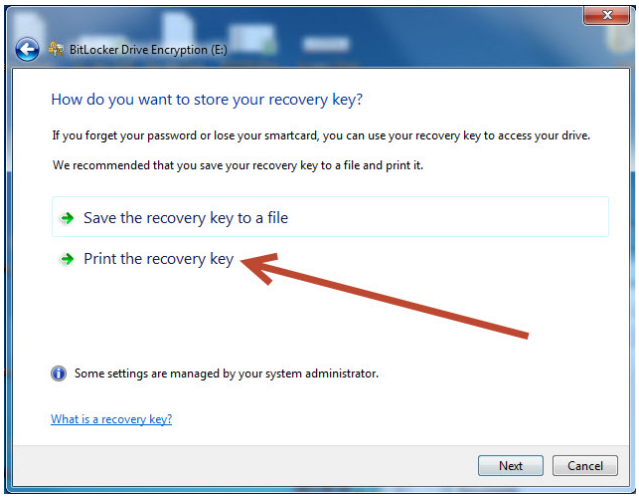
Right Click on the USB that you want to encrypt. Then **Click on "Turn on BitLocker"**.



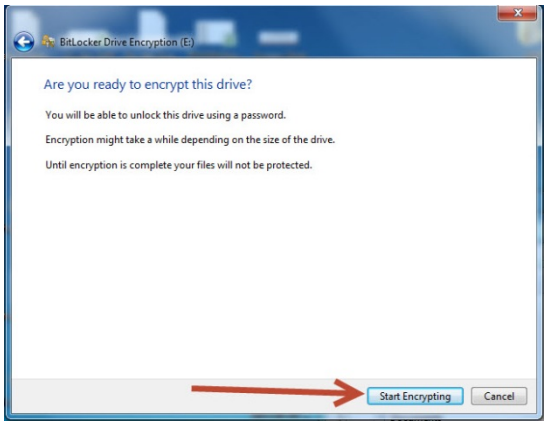
Select the box to "Use a password to unlock the drive" and **enter a strong password** that you will remember. A passphrase is usually a strong password containing at least 13 characters. An example of such a password could be: Thisisagreatpassword!



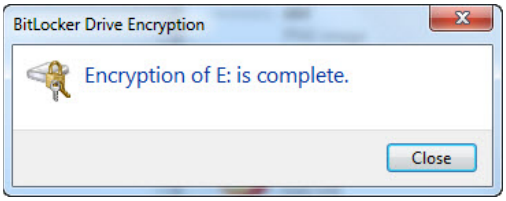
As a safety feature, to prevent you from forgetting the password and being locked out of your drive, you will be presented with recovery options. We recommend printing a recovery key and storing it in a safe location. If you forget your password and do not have your recovery key, **GRCC IT cannot recover your encrypted files.**



Click on "Start Encrypting" at which time the drive will begin encrypting. Do not remove the drive while it is encrypting.



When encryption is complete you will get a prompt which you can then close.



Next time you put your USB in a computer you will be prompt for the password which you must enter in order to access the USB and its contents.