SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-GDL-009-W7 – Encrypting Personal Computers (Windows 7)

Author: Paul Ferrier

Date: 14/10/2016

Document Security Level: **PUBLIC**
Document Version: 1.0
Document Ref: SEC-GDL-009-W7
Document Link:
Review Date: 01/11/2017

SEC-GDL-009-W7 – Encrypting Personal Computers (Windows 7)

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	03/06/2016 13:30	tbc	tbc	tbc
1.0	PF	ESA	Updated following peer review	14/10/2016 08:20			

Contents

SEC-GDL-009-W7 – Encrypting Personal Computers (Windows 7)

1. Introduction

Windows 7 offers users the ability to protect their files and folders with full disk encryption This means that if the hard drive is kept in the computer, or removed and connected to another computer the password or key will need to be supplied to be able to access the data stored on the hard drive.

Encrypting devices does not make them exempt from the DPA or the FOI act and hence you must be able to comply with the requirements to provide information, or the encryption key if required.

IMPORTANT
One word of caution, if you lose your encryption password or recovery key your data will be inaccessible. There are many ways to securely store your recovery key and these are detailed in section 3.4.

These guidelines provide the steps required to encrypt (and decrypt, if required) a personal computer running Windows 7.

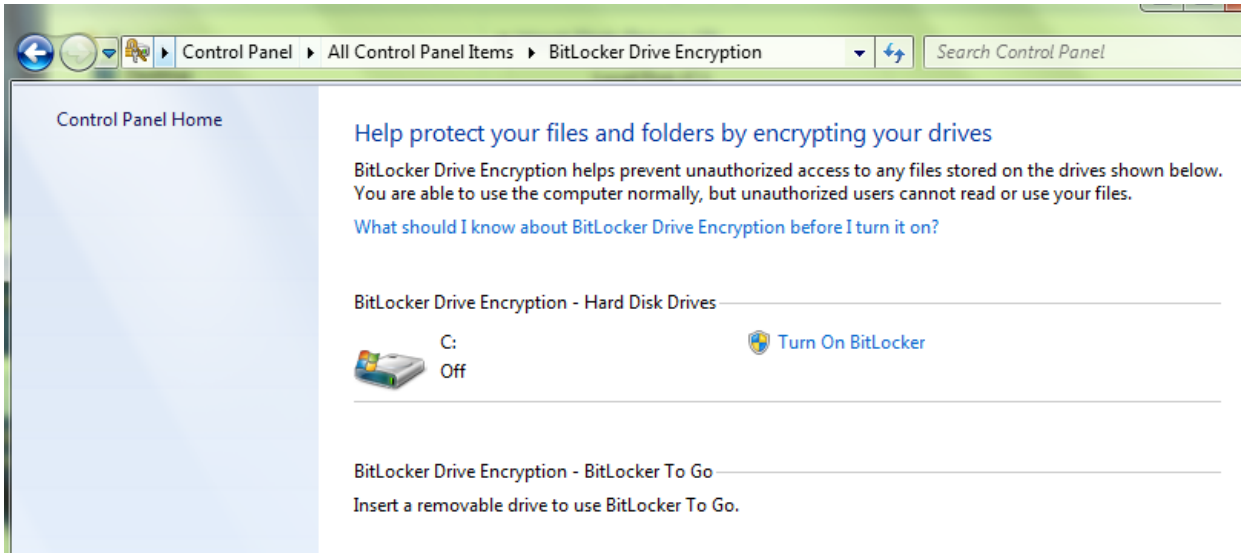
2. Quick check for hard drive encryption

If you are not sure whether your hard drive is encrypted, there is a simple way to check. Open File Explorer and look at your hard drives.

The image on the **left** depicts an **unencrypted hard drive** and on the **right** an **encrypted hard drive** (by virtue of the padlock and key).

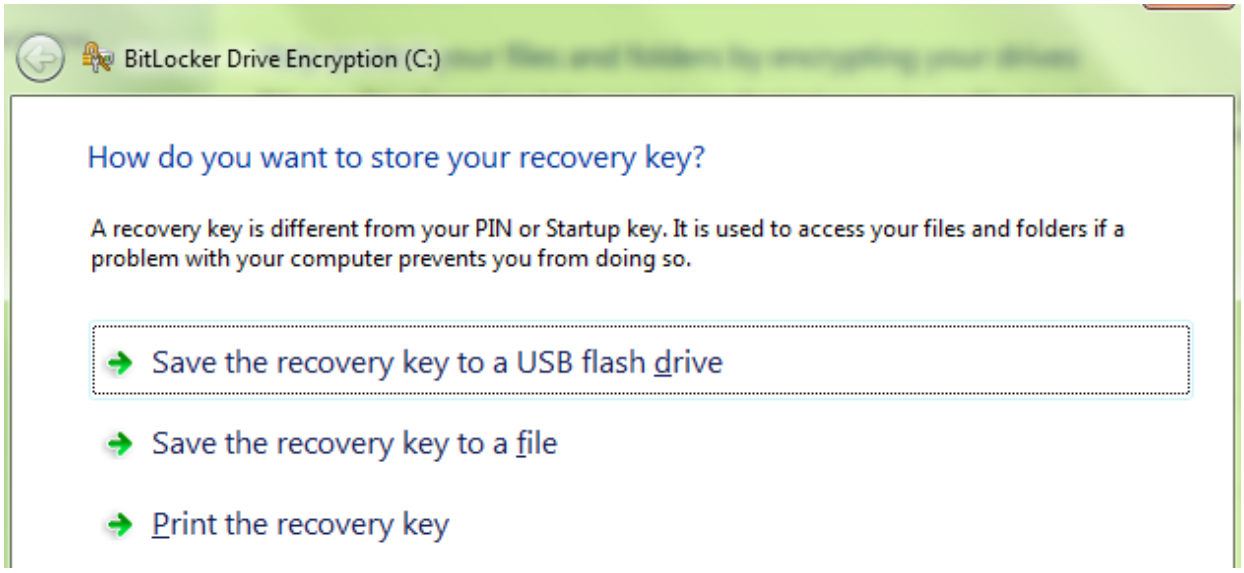
3. Encrypting a drive

3.1 In Windows Explorer, select the drive that you wish to encrypt and right-click it and select **Turn On BitLocker**; or using the **Control Panel** go to **System and Security** and **BitLocker Drive Encryption** (as shown over the page).

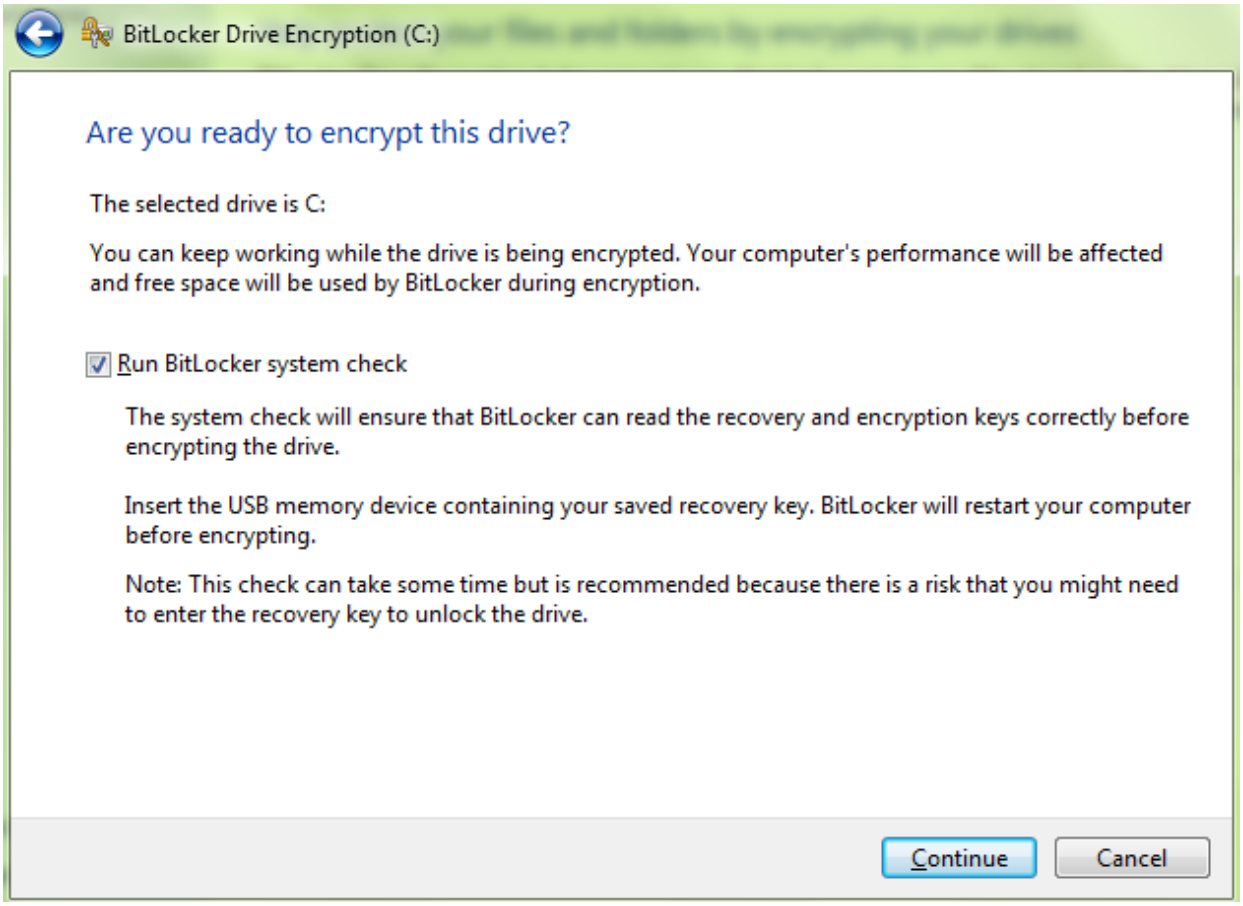


Select **Turn On BitLocker**.

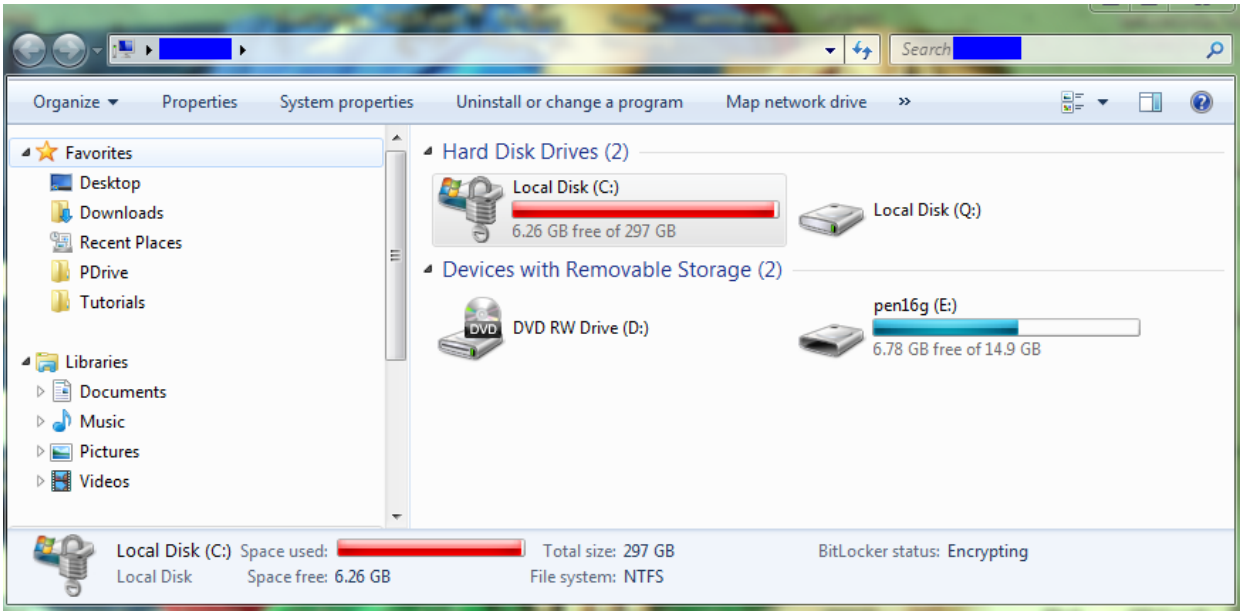
3.2 You are then presented with where you want to store your recovery key – this is important as it is required to be able to access the data on your computer. You have the ability to save it either to a USB stick or a file (**note**: this can't be stored on the hard drive you are about to encrypt) or it can be printed.



3.3 Once you have the recovery key somewhere safe, you can then progress with the encryption of the hard drive.

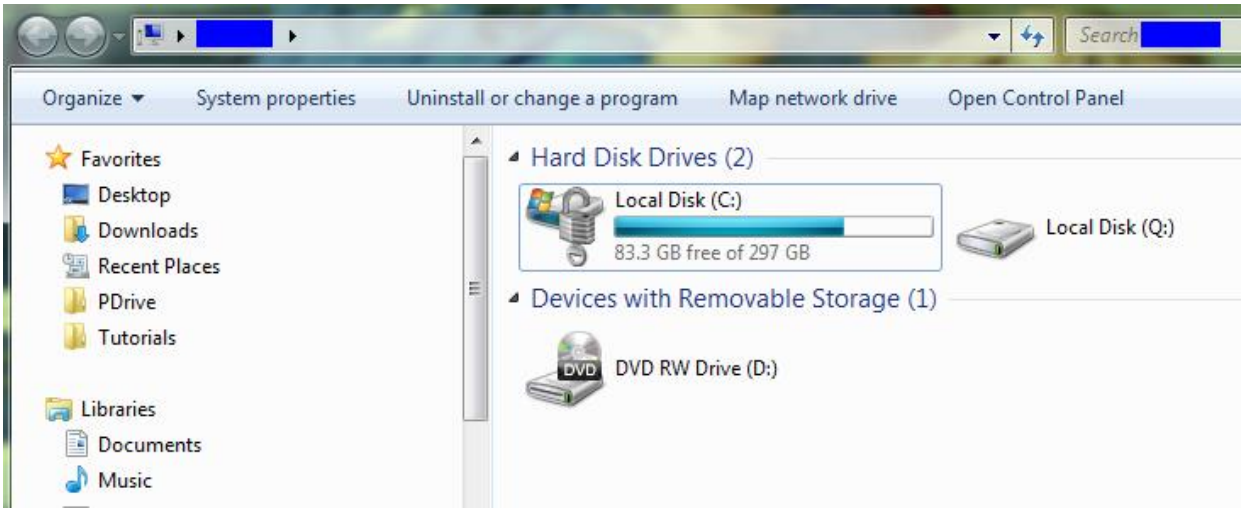


3.4 While your hard drive is encrypting you will still be able to use your computer, although you will notice that you have significantly less space on your hard drive throughout the encryption process.



3.5 Once the encryption is complete, the hard drive usage will revert to just above its pre-encryption level.

When you go back to Windows Explorer, you are presented with the padlock and key next to your drive icon.

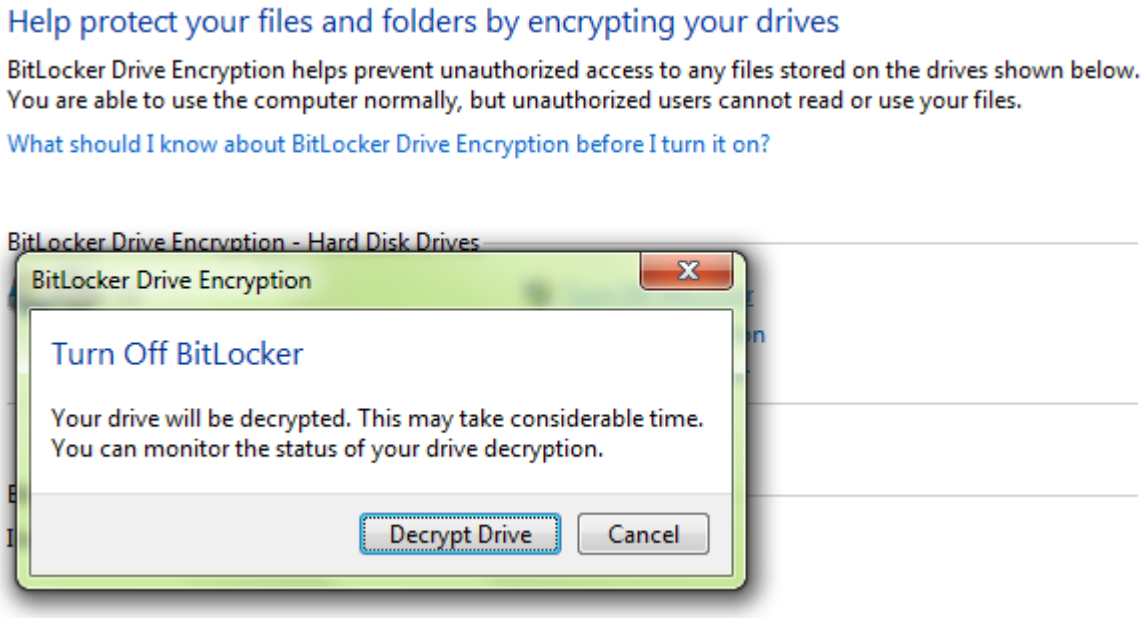


4. Decrypting a drive

4.1 Should you have the need to decrypt an encrypted hard drive, this is also really easy.

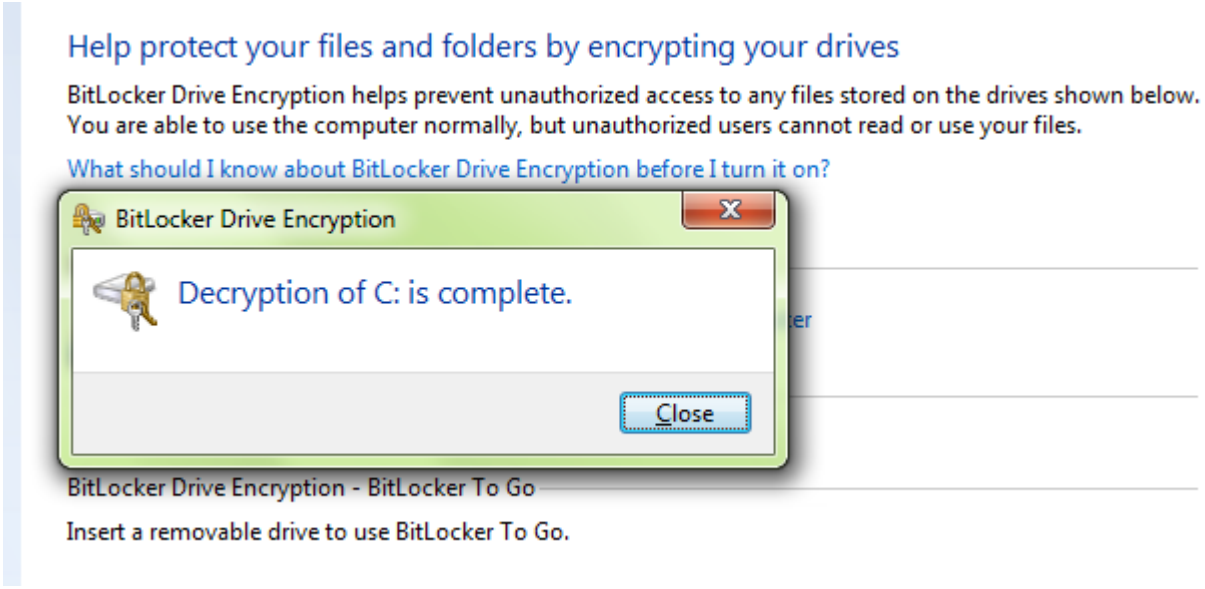
Either right click on the drive in question and select **Manage BitLocker**; or using the **Control Panel** go to **System and Security** and **BitLocker Drive Encryption** (as shown over the page).

When prompted, if this is what you intend to do, click the **Turn Off BitLocker** button.



4.2 You then need to click the Decrypt Drive button (shown above).

4.3 Once the decryption is complete, you will be notified. **Warning** at this time your information is one more only as secure as the device/hard drive that is in your possession, if you lose it, you are providing valuable information to a malicious user.


Help protect your files and folders by encrypting your drives
BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below.
You are able to use the computer normally, but unauthorized users cannot read or use your files.
What should I know about BitLocker Drive Encryption before I turn it on?
BitLocker Drive Encryption
Decryption of C: is complete.
Close
BitLocker Drive Encryption - BitLocker To Go
Insert a removable drive to use BitLocker To Go.