BitLocker

FAQ

Introduction

BitLocker Drive Encryption is a feature first introduced by Microsoft in Windows Vista, and helps to protect the confidential data on your computer from unauthorized access. BitLocker helps to ensure that sensitive information is not revealed should your computer be lost, stolen, or tampered with.

1. How does BitLocker protect my data?

Unlike many other encryption products that protect individual files, BitLocker Drive Encryption utilizes advance encryption standards to protect your entire hard drive. BitLocker can also encrypt and protect secondary hard drives, as well as USB thumb drives, to ensure the data they store is not improperly accessed.

In addition to data encryption, BitLocker is designed to utilize your computer's Trusted Platform Module (TPM) to monitor and protect critical firmware and operating system files from unauthorized tampering. If BitLocker detects that someone, or something, may be attempting to access your protected data, the encrypted drive is automatically locked and can only be accessed by providing a secret Recovery Key or password.

2. How can I use BitLocker to protect my Towson University computer?

Certain departments within the University have been identified as "High-Risk" due to their work with, and access to, confidential data. If you work in one of these departments, your computer may already have BitLocker Drive Encryption or a comparable encryption product installed and enabled and no further action is required.

If you are unsure if your computer is protected by BitLocker Drive Encryption, or if you work in a department not identified as "High-Risk" but wish to have your device encrypted, please contact the Faculty/Staff Help Center.

3. How can I use BitLocker to protect a USB drive?

When inserting a USB drive into a TU Faculty or Staff computer with BitLocker Drive Encryption enabled, you will be automatically prompted to encrypt the drive. When choosing to encrypt, you will be asked to create a password that will be required to access the drive when inserted into another computer.

Please note that if you choose to not encrypt the USB drive when prompted, you will be able to read its contents but unable to save any new data to it until it has been encrypted with BitLocker Drive Encryption.

OTS Publication: bl01 • 04/11/2019 • training@towson.edu