BitLocker – Staff and Faculty Usage

Scope: SO, CCC	**Revision date: 9/11/2020**
Approved by:	**Approved on date:**

Table of Contents

1. Introduction

The Connecticut State Colleges and Universities (CSCU) is securing the confidentiality of sensitive data on Connecticut Community College (CCC) and System Office (SO) owned laptop computers by implementing BitLocker Drive Encryption. Every content on a computer that ends up lost or stolen is vulnerable to unauthorized access, which can present a security risk to both yourself and CSCU. BitLocker provides protection for the operating system as well as the data stored on the computer; ensuring the data remains encrypted and inaccessible to unauthorized users. The configuration for BitLocker requires users to provide a PIN, in form of a password, to unlock the drive before making the operating system available for regular use.

It is important for you to understand the responsibility accompanied with a CCC or SO owned laptop encrypted with BitLocker. The standards listed in this documentation will provide a clear understanding and help set the proper expectations.

2. Purpose

This standard describes the strategy and responsibility for using BitLocker.

3. Scope

This standard applies to all faculty and staff at CCC institutions and the System Office.

4. Usage Provisions

The following are the BitLocker usage provisions:

- The usage of BitLocker is subject to all CSCU policies and standards, including the Acceptable Use Policy, the Information Security Policy and the Data Management Standard.
- Faculty and staff assigned or loaned a laptop must work with their local IT department or Helpdesk to create an enhanced PIN for BitLocker prior to receiving the laptop. Enhanced PIN simply means that you can create a PIN with numbers, letters, and special characters. The PIN you create is needed to unlock encryption on the laptop each time it is powered on and rebooted. Once unlocked, the Windows Operating System will prompt for your netID and password.
- The BitLocker PIN must contain a minimum of eight (8) characters in length
- All enhanced PINs must meet CSCU's Password Standard. The password requirements are summarized here.
- The BitLocker PIN cannot be the same as the current Windows password. Please, create a different combination. The PIN is not to be written down nor shared with anyone besides yourself. Doing so will result in a violation of CSCU's Acceptable Use Policy and put your information at risk.
- Unlike the Windows password, BitLocker does not require your PIN to be changed frequently. The initial PIN will remain as is unless changed by you.
- While signed into Windows, you can update the BitLocker PIN manually if you know the current PIN. If the PIN is forgotten, contact the local Helpdesk. Refer to the BitLocker End User Guide for instructions.
- If your laptop is lost or stolen, report it to the Helpdesk immediately.

5. Related Publications

Related Policies

- Acceptable Use Policy
- Information Security Policy

Related Standards & Procedures

- Data Management Standard

Web Sites

- Support Services Website

External links for Off-Site Users Regarding Travel

- Encryption FAQs (Bureau of Industry & Security, BIS)
- EAR Controls for Items That Use Encryption (Bureau of Industry & Security, BIS)
- FBI - Safety and Security Guidance for Traveling Abroad
- Department of State - Travel Alerts and Warnings
- Department of Homeland Security - "Know Before You Go" Resources
- Department of State - Websites of US Embassies Consulates, and Diplomatic Missions
- Department of State -"Smart Traveler Enrollment Program"

6. Revision History

History of Changes

- 8/31/2020: Original standard