VERMONT
STATE COLLEGES SYSTEM

Title	Policy ID:	
VSCS Laptop Full Disk Encryption Policy	628-1	
	Version:	Date:
	1.0	2018/12/06

1. Purpose

1.1. This policy defines the expectations of the full disk encryption technologies in use at the Vermont State Colleges System.

2. Scope

2.1. This policy applies to full disk encryption technologies in use at the VSCS.

3. Policy

3.1. VSCS IT staff deploy standard full disk encryption technologies to all VSCS provided laptops. Other systems may also employ the same full disk encryption technologies when deemed necessary for increased security due to factors such as location or function.

3.1.1. Exceptions may be made with documented approval from the VSCS CIO or a campus CTO. In such cases, other safeguards may be required to protect VSCS sensitive information in the event the device is lost (see 627-1_VSC_Information_Sensitivity_Policy for more information).

3.2. VSCS IT staff will install and configure full disk encryption software prior to delivering to the user. The VSCS central encryption server will maintain status information of encrypted devices at the VSCS. Local IT staff is responsible for updating to new versions of the encryption software and periodically reviewing encryption compliance.

3.3. Encryption software will be configured to:

3.3.1. Require a Pre-Boot Authentication key before booting into the operating system.

3.3.2. Periodically report status changes and encryption compliance to the VSCS central encryption server.

3.4. Full disk encryption technologies at the VSCS will be reviewed on a periodic basis to ensure currency and compliance with industry standards. All software for consideration will be minimally compliant with the requirements from NIST SP 800-175B and FIPS 140-2.

4. References

4.1. NIST SP 800-175B - Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

4.2. FIPS 140-2 - Cryptographic Module Validation Program

5. Definitions

5.1. VSCS – Vermont State Colleges System

6. Revisions

Date	Revision	Approval	Signature
2018/12/05	Draft	Donny Bazluke	
2018/12/06	Approved	IT Council	IT Council
2018/12/17	Approved	CIO - Kevin Conroy	Kevin Conroy