Standard: Device Encryption Standard

Effective Date:	2019.08.29
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Chief Information Officer
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The Device Encryption Standard describes the acceptable standards for encrypting data stored on university owned devices.

Who/what does the standard apply?

The requirements in this standard apply to any university owned device used for university business which contains Protected or Restricted data. Devices include, but are not limited to:

- Desktops
- Laptops
- Tablets
- Smartphones
- CD-ROM, DVD-ROM
- “USB Drives”, “Thumb Drives”, Flash media
- External hard drives

Definitions

- **Encryption:** The conversion of data into a form, called a ciphertext, which cannot be easily read by unauthorized people.
- **Restricted Data:** Information that is highly sensitive both externally and internally at the University. Unauthorized access could reasonably be expected to cause serious harm to individuals, businesses, other third parties or the University.
- **Protected Data:** Information that is sensitive externally and may be somewhat sensitive internally at the University. The inappropriate release of the information would reasonably be expected to cause minimal to moderate harm to individuals, businesses, other third parties or the University.
- **Public Data:** Information that is intended for, or is available to, the public

Compliance

University owned devices must align to the requirements and specifications outlined within this standard. Where systems are unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

Requirement	Specifications
Protected and Restricted University data stored on devices must be encrypted.	University provisioned devices must employ a University supported Encryption solution. Any mobile device must employ the Encryption solution that is native to the device where applicable.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Data Security Classification Guideline	
Use of Computer Facilities Policy and Procedure	