Standard: Use of Non-University Owned Devices

Effective Date:	2017.06.23
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 Use of Non-University Owned Devices Standard describes the acceptable standards for connecting to the University's networks or for accessing University Information with devices the University does not own.

Who/what does the standard apply?

The requirements in this standard apply to any non-university owned device accessing, processing, storing or transmitting University Restricted or Protected Information or connecting to the University's IT facilities via the wired or wireless network from a site on campus or remotely. Devices include, but are not limited to:

- Desktops
- Laptops
- Tablets
- Smartphones
- External Hard Drives or other storage devices.
- Any device not mentioned above, but where University data is stored. This may include virtual or cloud based storage services or devices.

Definitions

- **Encryption:** is the conversion of data into a form, called a cipher text, 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: I**nformation 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.
- **Logically Secured:** Preventing use of the device by an unauthorized person through the use of device features such as locking the screen, logging off the device, turning the device off.
- **Physically Secured:** Preventing access to the device or preventing removal of the device through physical constraints such as device cables, locked offices and cabinets

Compliance

Devices must align to the requirements and specifications outlined within this standard. Where a device is unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

Requirement	Specifications
Devices must meet University requirements when connecting to the University network.	Devices must have up-to-date operating systems installed that are still supported by the manufacturer. Devices must have up-to-date service packs and security patches installed.
Devices must be protected from viruses.	Where anti-virus software is available for a device it must be installed with the most up-to-date signatures.
3rd party software must be up-to-date.	3rd party software including but not limited to Java, Flash, Microsoft Office and Adobe Reader must have up-to-date security patches.
Devices must be protected from unauthorized access.	Devices must be password or PIN protected. Devices must be logically and physically secured when unattended.
Protected and Restricted University data stored on devices must be encrypted.	Devices must employ the Encryption solution that is native to or available for the device (i.e. using an encrypted USB).

References

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