Encryption Policy

Applies To:	All	**Policy Number:**	ITS-0043
Issued By:	AVP for IT	**Policy Version Number:**	1.0
Date Issued:	July 1, 2016	**Last Review Date:**	July 1, 2016
		Last Revised Date:	July 1, 2016

Scope

This policy covers all computers, electronic devices, and media capable of storing electronic data that house University Protected data or University Sensitive data as defined by the Data Classification Policy. This policy also covers the circumstances under which encryption must be used when data is being transferred.

Purpose

The purpose of this policy is to establish the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption.

Policy

Devices and Media Requiring Encryption

Encryption is required for all laptops, workstations, and portable drives that may be used to store or access University Protected data. Encryption is recommended for all laptops, workstations, and portable drives that may be used to store or access University Sensitive data. ITS will provide, install, configure, and support encryption where it is needed. Departments who have a laptop, workstation, or portable drive that needs to be encrypted should contact the ITS Helpdesk.

Electronic Data Transfers

Any transfer of unencrypted University Protected data or University Sensitive data must take place via an encrypted channel.

Encrypted University Protected data or University Sensitive data may be transmitted via encrypted or unencrypted channels. All email communications that involve email addresses outside of the University use an unencrypted channel, and therefore require that messages containing University Protected data or University Sensitive data be encrypted. Approved methods of encrypting electronic data transfers are listed in the appendix. If the encryption method includes a password, that password must be transferred through an alternative method, such as calling the individual and leaving the password on their voice mail. Email messages containing encrypted data may never include the password in the same message as the encrypted data. Individuals who are unsure if they are correctly encrypting electronic data transfers should contact the ITS Helpdesk.

Physical Transfer of Electronic Data

Any time University Protected data or University Sensitive data is placed on a medium such as a CD, DVD, or portable drive to facilitate a physical transfer, either entirely within the University or between the University and a 3rd party, that data must be encrypted. Archiving University Protected data or University Sensitive data to a physical medium is not

recommended, but is permitted if the data is encrypted. All archiving should be done electronically, so that it is stored in a controlled data center and backed up by ITS.

Software

ITS will install software that is capable of encrypting the entire hard drive on all identified University computers and electronic devices subject to this Policy. Users who require encryption software should contact ITS to arrange installation of encryption software.

History and Updates

July 1, 2016: Initial Policy