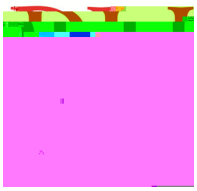

Information Technology Policy and Procedures

Policy: Encryption

Policy Title: Encryption Policy	**Last Review Date: 5/18/2020**
Policy ID: 5100	**Effective Date: 2/3/2009**
Oversight Executive: VP for Information Technology & CIO	**Review Date: 5/1/2021**

1. Purpose

The purpose of this policy is to secure highly sensitive (sensitive) University data. Encrypting sensitive information helps protect against data exposure if the storage device is lost or stolen and against some types of unauthorized physical access to the device. Encrypting sensitive data in transit protects against other kinds of threats including "sniffing" and "man-in-the-middle" attacks.

2. Policy

Transmission

All transmission of sensitive data requires the use of appropriate encryption. Files can be encrypted before they are transmitted across the network (as an email attachment) for example. This can be used as an alternative to encrypting the transmission channel.

Data Storage Media

It is prohibited to store sensitive data on any non-network storage device or media, unless the data is encrypted and there is a written exception approved by the agency head or designee. Prohibited storage media includes storage on desktop computers, laptop computers, PDA's, cell phones, USB drives, thumbdrives, memory cards, CD's, DVD's and other USB devices (e.g. media players, cameras, etc.) 4

Encryption technologies (applications, protocols, and algorithms) mu
Officer (ISO). Other unapproved or proprietary encryption algorithm
This includes any proprietary encryption that has not been made pub

Key Recovery

For data

of record, where the only access to it is available by decryption, copies of the keys must be burned to a labeled CD and placed in a sealed labeled envelope, or the password for approved software must be written and placed in a sealed labeled envelope. In either case the envelope shall be presented to the ISO for key recovery purposes. Whenever a password change

storing sensitive information to the ISO. Sensitive data that is properly stored on a network share or device will not be mirrored to the local device (as with "offline files and folders").

4.