RU
RADFORD
UNIVERSITY

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.)

3. Procedures

Allowed Encryption

Encryption technologies (applications, protocols, and algorithms) must be approved by the Information Security Officer (ISO). Other unapproved or proprietary encryption algorithms are not sufficient to meet this standard. This includes any proprietary encryption that has not been made public and/or has not withstood public scrutiny.

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 occurs for data of record the old key/password information must be retrieved, destroyed and replaced with the new key/password information by contacting the ISO. Appropriate identification will be required for all transactions.

Exceptions

An exception must be granted in writing from the agency head or designee to allow sensitive data to be stored on any non-network storage device, even when encrypted. Contact the ISO for more information on exception approval. Sensitive data may be stored on properly administered University network share devices including the "H: drive". Departments must provide information regarding the existence, setup and administration of devices

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. Definitions

Highly Sensitive Data: University data which, because of its potential risk in the event of disclosure, alteration or destruction, is approved for use only on a very limited basis and with special security precautions. This includes personally identifiable information that can lead to identity theft exposure.

5. Related Information

IT-5102 Data Storage and Media Protection
IT-5102s Data and System Classification Standard
IT-5003s IT Security Standard

6. Policy Background

7. Approvals and Revisions

Approved: June 30, 2007 by Vice President for Information Technology & CIO

Revised: July 1, 2008
Minor changes for clarification
Approved: July 1, 2008 by Vice President for Information Technology & CIO

Revised: February 1, 2009
Policy renumbered to Information Technology Policy 5100 from former Information Technology Policy 105.
Updated to include changes to Virginia Information Technologies Agency Security Policy 501.
Approved: February 1, 2009 by Vice President for Information Technology & CIO

Review: November 12, 2018
Minor wording changes for clarification.

Revised: May 18, 2020
Updated definitions.