



Information Technology Policy and Procedures

Policy: Encryption

Policy Title: Encryption Policy	Approval Date: 2/3/2009
Policy ID: 5100	Effective Date: 2/3/2009
Oversight Executive: VP for Information Technology & CIO	Review Date: 2/3/2010

1. Purpose

The purpose of this policy is to secure sensitive Commonwealth of Virginia (COV) data and comply with COV state policy.

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 unencrypted 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 Radford University Information Security Officer (RU 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 RU ISO for key recovery purposes. When ever 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 RU ISO. Appropriate identification will be required for all transactions.



Information Technology Policy and Procedures

Policy: Encryption

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 RU ISO for more information on exception approval. Sensitive data may be stored on properly administered COV owned network share devices including the "H: drive". Departments must provide information regarding the existence, setup and administration of devices storing sensitive information to the RU ISO. 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

Sensitive Data

Sensitive data, according to VITA, is data which, if compromised with respect to confidentiality, integrity, or availability, could adversely affect COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. For example: social security numbers, drivers license or identification card numbers, financial account numbers, and credit or debit card numbers are considered sensitive data. Other items may also be defined as sensitive in other policies or legislation including FERPA and HIPAA for example.

Directory information is not considered sensitive.

5. Related Information

Authority

VITA's SEC501 policy states:

"Commensurate with sensitivity and risk, each agency shall... Require encryption during transmission of data that is sensitive relative to confidentiality or integrity..." and "Prohibit the storage of sensitive data on any non-network storage device or media... unless the data is encrypted and there is a written exception approved..."

6. Policy Background

7. Approvals and Revisions

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

Revised: 7/1/2008

Minor changes for clarification

Approved: July 1, 2008 by Vice President for Information Technology & CIO

Revised: 2/1/2009

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