Purpose

This policy reflects the University's commitment to protect University data from improper or unauthorized disclosure. The purpose of this policy is to also ensure that the VSU Technology Services department implements appropriate data storage and media protection procedures, encryption technologies and manages cryptographic keys to protect data from compromise.

Authority, Responsibility, and Duties

The IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as, the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Refer to Information Security Policy 6110 for roles and responsibilities

A. VSU Information Security Officer (ISO)

The VSU ISO, in collaboration with the VSU Chief Information Officer (CIO) and VSU Data Center Manager, is responsible for the management of Data Storage Media Protection and Encryption processes for the University.

B. Technology Services

Members of the VSU Technology Services department will be assigned responsibilities for documenting and implementing Data Storage Media Protection and Encryption procedures commensurate with sensitivity and risk.

Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

Policy Statements

1. This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who develop and use VSU information technology resources to conduct University business and to transmit sensitive data or personally identifiable information (PII) in the performance of their jobs, and all VSU information systems that store or process PII or other sensitive data.
2. Implementation and management of data storage media protection, encryption and cryptographic key management must comply with applicable laws, directives, policies and standards, and at a minimum includes:
   A. Define protection of stored sensitive data as the responsibility of the Data Owner.
   B. Technical procedures are established and enforced to police and prohibit the storage of

Sensitive data on any non-network storage or media (except for backup media) unless the data is encrypted. There is a written exception approved by the ISO in accordance with the VSU exception process.

C. ·Prohibit the storage of sensitive data on local hard drive or any non-network storage device or media, except for backup media, unless the data is encrypted.

D. Prohibit the storage of any Commonwealth data on IT systems that are not under the contractual control of the Commonwealth of Virginia (COV). The owner of the IT system must adhere to the latest COV auditing and standards.

E. Prohibit the connection of non-COV owned or leased data storage media or devices to a COV-owned or lease resource, unless connecting to the guest network or guest resources.

F. Logical and physical protection is required for all data storage media containing sensitive data, commensurate with sensitivity and risk.

G. The auto-forwarding of emails to external accounts is prohibited to prevent data leakage unless there is a documented business case and written exception approved by the ISO in accordance with VSU exception process, which clearly identifies residual risks.

H. Forwarding of private, VSU documents from the user's VSU email address to the user's private email address is prohibited.

I. The pickup, receipt, transfer, and delivery of all data storage media containing sensitive data is restricted to authorized personnel in the University's Data Center.

J. Procedures to document and safeguard handling of all backup media containing sensitive data is implemented, using encryption when data is sensitive relative to confidentiality and/or, if encryption is not an option, implement and document mitigating controls and procedures.

K. Restrict access to digital and non-digital media to authorized individuals using organization-defined security measures.

L. Processes must be implemented to sanitize data storage media prior to disposal or reuse in accordance with (COV) Information Technology Resource Management (ITRM) Standard Sec. 514, Removal of Commonwealth Data from Surplus Computer Hard Drives and electronic Media.

M. Practices must be defined and documented for selecting and deploying encryption technologies and for the encryption of data.

N. Appropriate processes must be documented before implementing encryption that include at a minimum the following:

   I. Instructions in the Security Incident Response Plan on how to respond when encryption keys are compromised;

   2. A secure key management system for the administration and distribution of keys; and

   3. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss.

O. Encryption is required for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publically accessible networks, or any transmission outside of the data's broadcast domain.

P. Digital signatures may be deployed for data that is sensitive relative to integrity

Q. Sensitive documents being emailed off of the VSU.edu domain must be encrypted to protect the confidentiality of the data.

References

Virginia Information Technology Agency (VITA):
Information Security Standard (SEC 501-09) (02/20/2015)
Removal of Commonwealth Data from Surplus Electronic Media Standard (SEC 514-04) (12/21/2015)

Approval By: _____ Date: 5/10/16
President