Title: Data Storage Media Protection and Encryption Policy Policy: 6400

Purpose

The University is committed to protecting University data from improper or unauthorized disclosure. Therefore, the VSU Technology Services department implements appropriate data storage and media protection procedures, encryption technologies, and manages cryptographic keys to protect data from compromise. This policy includes systems directly supported by VSU's Technology Services Team and systems that may be hosted by a service provider. VSU understands their authority and responsibility of ensuring that its service providers are governed by and adhere to the same Commonwealth Security Standards and VSU Policies, as the University.

Authority, Responsibility, and Duties

The 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.

A. Information Security Officer (ISO)

The ISO, in collaboration with the Chief Information Officer (CIO) is responsible for the management of Data Storage Media Protection and Encryption processes for the University. Both, ISO and CIO, should understand the technology options to adequately protect data in-transit and at rest and records retention requirements for various data types. The ISO, System Owners and Data Owners should work together to ensure that the University's data and information assets are protected.

B. System Owners

System Owners are responsible for understanding the type of data that is resident in the systems under their direct purview. The System Owner, Data Owner and the ISO will collaborate to ensure that data requirements are understood and controls are in place to protect data in-transition and at rest. The System Owner should also understand the data retention requirements for all systems they oversee.

C. Data Owners

Data Owners are responsible for understanding the data requirements and restrictions for the data under their governance. (A special focus is given to the protection of stored sensitive data.) Collaboration with System Owners, ISO and Enterprise Manager is expected in order to fulfil the responsibly of adequate data stewardship.

D. Enterprise Manager

The Enterprise Manager and the Enterprise Management team are responsible 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:

   A. Ensures that Data Owners are aware of, and trained in, their responsibilities for the protection of stored sensitive data.

   B. Ensures 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. Prohibits storage of any Commonwealth or University data on IT systems on local hard drives and/or provide encryption technologies.

   D. Prohibits the storage of any Commonwealth data on IT systems that are not under the contractual control of the Commonwealth of Virginia. The owner of the IT System must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.

   E. Prohibits the connection of any non-COV owned or leased data storage media or device to a COV-owned or leased resource, unless connecting to a guest network or guest resources. This prohibition, at the University's discretion need not apply to an approved vendor providing operational IT support services under contract.

   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. The pickup, receipt, transfer, and delivery of all data storage media containing sensitive data is restricted to authorized personnel.

   I. Physically controls and securely stores digital and non-digital media within organization-defined controlled areas using organization-defined security measures;

   J. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

   K. 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.

   L. Processes must be implemented to sanitize data storage media prior to disposal or reuse in accordance with Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Standard SEC514-04 (12/21/15), Removal of Commonwealth Data from Electronic Media Standard.

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:

1. 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. Protects and controls digital and non-digital media during transport outside of controlled areas using organization-defined security measures;

R. Maintains accountability for information system media during transport outside of controlled areas;

S. Documents activities associated with the transport of information system media; and

T. Restricts the activities associated with the transport of information system media to authorized personnel.

References

Virginia Information Technology Agency (VITA):

Information Security Standards (SEC501-09.1) (12/08/2016)
IT Systems Security Guideline (SEC515-00) (7/17/2008)
Removal of Commonwealth Data from Electronic Media Standard (SEC 514-04) (12/21/2015)

9/6/17

Approval By: ________________________ **Date:** ________________

President