



OIT 62.602: Data Storage Media Protection

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

Data Protection provides security safeguards for the processing and storing of data. This component outlines the methods that the University can use to safeguard the electronic information, irrespective of medium, in a manner commensurate with the sensitivity and risk of the information stored.

II. Purpose

The Data Storage Media Protection policy identifies the steps necessary for the appropriate handling of stored data to protect the data from compromise.

III. Scope

This policy applies to NSU employees and other personnel (i.e. supporting vendors, consultants, etc.) who have access to sensitive and confidential University information.

IV. Requirements

NSU shall or shall require that its service provider document and implement Data Storage Media Protection practices. At a minimum, these practices must include the following components:

1. Define protection of stored sensitive data as the responsibility of the Data Owner.
2. Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head accepting all residual risks. The exception shall include the following elements:
 - a. The business or technical justification;
 - b. The scope, including quantification and duration (not to exceed one year);
 - c. A description of all associated risks;

- d. Identification of controls to mitigate the risks, one of which must be encryption; and
- e. Identification of any residual risks.

Note: Non-network storage device or media, includes removable data storage media and the fixed disk drives of all desktops and mobile workstations, such as laptop and tablet computers, USB drives, CDs, etc.

- 3. Prohibit the storage of any Commonwealth data on non-COV issued computing devices. This prohibition, at the University's discretion need not apply to Internet-facing web sites serving non-sensitive data. University contactors may store non-sensitive COV data for the execution of the University contract. This requirement is due to records retention and Freedom of Information Act (FOIA) complexities, as well as the associated information security risks.
- 4. Require logical and physical protection for all data storage media containing sensitive data, commensurate with sensitivity and risk.
- 5. Prohibit the connection of any non-University owned data storage media or device to a University-owned 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.

Note: Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, desktops, laptops, and digital music players owned by employees, contractors, and students.

- 6. Prohibit the auto-forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing residual risk approved in writing by the Agency Head.
- 7. Restrict the pickup, receipt, transfer, and delivery of all data storage media containing sensitive data to authorized personnel.
- 8. Procedures must be implemented and documented to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered where the data is sensitive as related to confidentiality. Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.
- 9. Implement processes to sanitize data storage media prior to disposal or reuse.

Note: The University and any service provider should implement procedures to instruct Administrators and users on the disposal of data storage media when

no longer needed in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.