Policy Title: Media Storage

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1004 (2014) Media Storage

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Media storage policies encompass the storage rules for any data or medium for storing data, whether sensitive or otherwise, and is accordingly necessary to assist in maintaining data integrity within the University’s information system.
PURPOSE

This control is intended to establish the policy and procedures for media storage on the University’s information system.

REQUIREMENTS

NSU:

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

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

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.

Supplemental Guidance: The strength of mechanisms is commensurate with the classification and sensitivity of the information.

Control Enhancements for Sensitive Systems:

1. NSU employs cryptographic mechanisms to protect information in storage.

Enhancement Supplemental Guidance: Requires documented approval from the agency head.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 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.

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.
PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:

  - Supersedes (previous policy): OIT 62.8.1004 Media Storage

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard