UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38-01 (2020) Media Protection Policy

Policy Title:	Media Protection Policy
Policy Type:	Board of Visitors
Policy Number:	BOV #38-01 (2020)
Approval Date:	December 11, 2020
Responsible Office:	Office of Information Technology (OIT)
Responsible Executive:	Vice President for Operations and Chief Strategist for Institutional Effectiveness
Applies to:	All Norfolk State University (NSU) employees (classified, hourly, official representatives, and third party vendors)

POLICY STATEMENT

The Media Protection policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with the responsibility to implement media protection controls. This policy defines information security requirements that ensure device and media protection during the storage, transport, and disposal of Information Resources.

This policy also meets the control requirements outlined in Commonwealth of Virginia Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC501, Section 8.10 Media Protection Family, Controls MP-1 through MP-6, to include specific requirements for the Commonwealth of Virginia.

TABLE OF CONTENTS **PAGE NUMBER**

DEFINITIONS

Chief Information Officer (CIO): Oversees the operation of NSU Information Technologies. Responsible for policies, procedures, and standards for assessing security risks, determining the appropriate security measures and performing security audits.

Data Classification: A process of categorizing data according to its sensitivity.

Data Owner: An individual, who defines, manages and controls the use of data and ensures compliance with adopted standards within NSU.

Data Storage Media: A device used to store data. Examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

Director of IT Security (DIS): The senior management designated by the CIO of NSU to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of information systems and data.

Office of Information Technology (OIT): The Office of Information Technology (OIT) manages the administrative and academic information technology resources for Norfolk State University.

Sensitivity Classification: The process of determining whether and to what degree information systems and data are sensitive.

Sensitive Data: Any data of which the compromise, with respect to confidentiality, integrity, and/or availability, could adversely affect NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled.

System Owner: A NSU Manager designated by the Agency Head or Information Security Officer, who is responsible for the operation and maintenance of an agency IT system.

System Administrator: An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner.

CONTACT(S)

The Office of Information Technology officially interprets this policy. The Chief Information Officer is responsible for obtaining approval for any revisions as required by BOV Policy #1 (2014) *Creating and Maintaining Policies* through the appropriate governance structures. Questions regarding this policy should be directed to the Office of Information Technology, (757) 823-2916.

STAKEHOLDER(S)

All NSU Faculty, Staff, Students, & Community.

MEDIA PROTECTION POLICY

OIT will develop, disseminate, and review and update the Media Protection Policy on an annual basis to prevent unauthorized use or misuse of NSU data and promote the privacy and security of sensitive information within NSU and its customers, in accordance with SEC501, MP-1 through MP-6.

A. MEDIA PROTECTION POLICY AND PROCEDURES

1. The DIS or designee shall document and implement Data Storage Media protection practices. At a minimum, these practices must include the following components:
   a. Define the protection of stored sensitive data as the responsibility of the Data Owners.
   b. 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 CIO accepting all residual risks.
      - The exception shall include the following elements:
        1. The business or technical justification.
        2. The scope, including quantification and duration (not to exceed one year).
        3. A description of all associated risks.
        4. Identification of controls to mitigate the risks, one of which must be encryption.
        5. Identification of any residual risks.
   c. Prohibit the storage of any NSU data on IT systems that are not under the contractual control of the Commonwealth of Virginia or Norfolk State University. The owner of the IT System must adhere to the latest NSU and Commonwealth of Virginia information security policies and standards as well as the latest applicable auditing policies and standards.
   d. Prohibit the connection of any non-NSU owned or leased data storage media or device to a NSU-owned or leased resource, unless connecting to a guest network or guest resources. This prohibition, at the discretion of NSU, need not apply to an approved vendor providing operational IT support services under a contract.
      - NSU employees are allowed to bring personal IT assets onto NSU or business partner premises that house NSU systems and data although personal IT assets may not be connected to the NSU or business partner network unless logical separation is utilized.

e. 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 CIO.

B. **MEDIA ACCESS**

1. The DIS or designee shall require that access to digital and non-digital media is restricted to authorized individuals only, using NSU-defined security measures.

   Note: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

2. Assessment of risk must guide the selection of media, and associated information contained on that media requiring restricted access.

3. System Owners must document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures are taken to restrict access.

C. **MEDIA STORAGE**

1. The System Owner or designee shall implement and document procedures to safeguard the handling of all backup media containing sensitive data. At a minimum, these procedures must include the following requirements:

   a. Employing cryptographic mechanisms to protect the information in storage 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;

      - The strength of mechanisms is commensurate with the classification and sensitivity of the information.
      - Encryption requires documented approval from the CIO.

   b. Physically controlling and securely storing digital and non-digital media within NSU-defined controlled areas using NSU-defined security measures; and

   c. Protecting information system media until the media are destroyed or sanitized using approved technology, techniques, and procedures.

D. **MEDIA TRANSPORT**

1. The DIS requires that:

a. All digital and non-digital media is protected and controlled during transport outside of controlled areas using NSU-defined security measures (i.e., locked container, cryptography).
   - NSU employees are responsible for safeguarding any IT assets they remove from NSU or business partner premises, including keeping these assets under their direct physical control whenever possible, and physically securing the assets (i.e., by means of lock and key) when they are not under the employee's direct physical control.

b. Accountability for information system media is maintained during transport outside of controlled areas.
   - NSU employees must immediately report loss or theft of any IT assets assigned to them to their supervisor and to the DIS.

c. Activities associated with the transport of such media are restricted to authorized personnel.
   - NSU employees shall not remove NSU or business partner owned IT assets from company premises.
     1. One exception to this policy is IT assets assigned to employees to include laptop computers, cellular telephones, and Personal Digital Assistant (PDA) devices.

2. The DIS or designee shall document, using established documentation requirements, activities associated with the transport of information system media in accordance with NSU assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.

   a. At a minimum, any log or tracking mechanism must include:
      - Description of information being transported
      - Type of information (e.g., PII) contained on the media
      - Method(s) of transport
      - Protection measures employed
      - Name(s) of individual(s) transporting the information (if appropriate)
      - Authorized recipient(s)
      - Dates sent and received

b. In instances where it is necessary to remove or transport sensitive document(s) or media outside of controlled areas of NSU, DIS approval must be obtained and documented.

c. Before transporting, delivering, or mailing media containing sensitive information, individuals shall:

- Notify the entity authorized to receive the information
- Document the following information:
  1. An identifying document number, if used
  2. Description of the information
  3. Name and signature of the sender
  4. Date sent

d. Media containing sensitive information transported by a common carrier must use an acknowledgment of receipt.

e. Personnel transporting sensitive information by car shall store the media in a locked trunk while in route.

- If a trunk is not available in the vehicle, the media must be hidden from sight.
- Personnel are prohibited from leaving media containing sensitive information in a vehicle overnight.
- If media containing sensitive information is being transported and delivered by hand, then it must be given directly to the recipient or another authorized individual.

3. The System Owner shall employ an identified custodian throughout the transport of sensitive information system media.

   a. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

4. Approved cryptographic mechanisms must be employed to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

   Note: This requirement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones).

E. MEDIA SANITIZATION

1. The DIS requires that information system media, both digital and non-digital, is sanitized prior to being disposal of, released out of NSU control, or released for reuse.
   a. Media sanitization and disposal actions must be tracked, documented, and verified.
   b. Sanitization technology and procedures must be tested to verify correct performance in accordance with the current version of the Removal of Commonwealth Data from Electronic Media Standard (COV ITRM Standard SEC514).
   c. Sanitization of portable, removable storage devices must be completed prior to connecting such devices to the information system.
   d. Sanitization of portable, removable storage devices, must be considered when:
      - Such devices are first purchased from the manufacturer or vendor prior to initial use.
      - When NSU loses a positive chain of custody for the device.
   e. An assessment of risk must guide the specific circumstances for employing the sanitization process.
   f. Information system media must be destroyed that cannot be sanitized.
   g. Removal of data from IT assets must be completed prior to disposal in accordance with the current version of the Removal of Commonwealth Data from Electronic Media Standard (COV ITRM Standard SEC514).
      - Data Owners of data residing on NSU owned or leased hard drives and electronic media will perform, or cause to be performed, the following procedures:
        1. Before the removal process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.
        2. The method used for removal of NSU and NSU Customer data, depends upon the operability of the hard drive and or electronic media.
        3. Whenever licensed software is resident on any electronic media being surplused, transferred, traded-in, disposed of, or replaced, the terms of the license agreement shall be followed.
        4. Operable hard drives and or electronic media that will be reused must be overwritten prior to disposition. If the hard drive and or electronic

media is removed, is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

5. Deleting files or using the format command does not prevent data from being recovered by technical means, and therefore it is **not** an acceptable method of removing data from NSU owned or leased hard disk storage media.
6. Electronic media shall be securely erased at the earliest time after being taken out of use but not later than 60 days.
7. The effectiveness of the data removal process shall be tested by a quality assurance function independent of the OIT team performing the data removal.

2. One of the following three acceptable methods shall be used for the removal of data from hard drives:

   a. Overwriting – Overwriting is an approved method for the removal of NSU data from hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented.

      - The overwriting process including the software products and applications used for the overwriting process shall include the following steps:

        1. The data shall be properly overwritten with pseudo-random data by means of, at a minimum, one pass of the entire device for a 15 gigabyte or greater drive. A minimum of three passes of pseudo-random data must be applied to drives smaller than 15 gigabytes in size.
        2. The software shall have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.
        3. The software shall have the capability to overwrite using a minimum of one pass or three passes of pseudo-random data on all sectors, blocks, tracks, and any unused disk space on the entire disk medium.
        4. The software or supporting software shall have a method to verify that all data has been removed. Verification must be performed to verify that each drive overwritten is, in fact, clean of any intelligible or prior data. This verification can be either as a separate process or included as part of the software used for overwriting.

5. Sectors not overwritten shall be identified and if they cannot be removed overwriting is not acceptable and another method must be employed.

b. Degaussing – A process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.

- Hard drives and or electronic media cannot be used after degaussing. The degaussing method will only be used when the hard drive and or electronic media is inoperable and will not be used for further service.

Note: Extreme care should be used when using degaussers since this technology can cause extreme damage to nearby telephones, monitors, and other electronic technology. Also, the use of a degausser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts will be audited periodically to detect technology or procedure failures.

c. Physical Destruction – Hard drives should be physically destroyed when they are defective, cannot be economically repaired, no longer meet minimal operating requirements or NSU data cannot be removed for reuse. Physical destruction must be accomplished to an extent that precludes any possible retrieval of data contained on the hard drive.

- Hard drives shall be destroyed in accordance with COV Standard SEC514.

3. Electronic devices that hold user data or configurations in non-volatile memory shall have all NSU data removed by either the removal of the battery or electricity supporting the non-volatile memory or by such other method recommended by the manufacturer for devices where the battery is not removable. This is to include all computer technology that has memory such as personal computers, PDAs, routers, firewalls, and switches.

4. If there is any risk of disclosure of sensitive data on media other than hard drives or devices that hold user data or configurations in non-volatile memory, that media should be overwritten, degaussed or destroyed. Disintegration, incineration, pulverization, shredding or melting are acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.

5. The effectiveness of the data removal process shall be tested by a quality assurance function independent of the team performing the data removal. The quality assurance tester shall test for effective data removal for electronic media once the data has been removed or otherwise made unreadable. If more than one device has had the data

removed, a sample of each device type can be tested as opposed to testing every device. The sample should include each type of electronic media (i.e., hard drives of personal computers, Personal Digital Assistants (PDAs), routers, firewalls, switches, tapes, diskettes, CDs, DVDs, worm devices, printers, and Universal Serial Bus (USB) data storage devices). The sample size for each device type should be commensurate with the sensitivity and risk of the type of data stored but must be at least 10% of the total number of devices for each type of electronic media.

a. The testing must be documented including date, tester(s), the total number of devices in the lot, number tested, method of testing and the result. Testing must be performed within 1 week of data removal. Test methods may include physical observation if the data removal method was physical destruction or attempting to boot up and read data if the method was overwriting.

6. NSU will audit the removal of data for compliance with this policy and procedure when any computer hard drives or electronic media are made surplus, transferred, traded-in, disposed of, or the hard drive is being replaced to ensure the audit process occurs in a timely manner, and the audit controls are effective.

   a. The removal of NSU data must be performed and documented as required in the Commonwealth of Virginia ITRM Standard (SEC514).

   b. The certification form must be completed and a copy affixed to the hard drive as required in the Commonwealth of Virginia ITRM Standard (SEC514).

7. Recommended software for the removal of commonwealth data from hard drives and electronic media are covered in the Commonwealth of Virginia ITRM Standard (SEC514).

8. If recovery of data contained on an electronic storage media is required, OIT or its service provider must provide adequate controls commensurate with the sensitivity of the data contained on the storage media as follows:

   a. If a third party is used to recover the data, OIT must ensure that the work is performed in accordance with the requirements for data protection as outlined in NSU's security program policies.

   b. NSU may require a non-disclosure agreement and/or confidentiality agreement in order to strictly enforce the privacy of the data.

   c. If the media must be removed from NSU's premises and sent offsite for recovery, NSU must ensure that the vendor provides a secure facility and safeguarding capabilities such as background checks, etc. to address handling and processing requirements of sensitive information.

9. NSU or its service provider shall make considerations in new or renewed contracts that address the protection of NSU data on hard drives for warranty or maintenance purposes. Following are standards when maintenance or warranty is necessary:
    a. If the hard drive malfunctions and data can be removed in accordance with the requirements in this policy, the drive may be returned to the supplier for replacement under warranty or maintenance.
    b. Hard drives that are inoperable and do not allow data to be removed in accordance with the requirements in this standard, shall be physically destroyed using a method previously outlined.

EDUCATION AND COMPLIANCE

A. SECURITY POLICY TRAINING

Security policy training is intended to educate NSU employees who have a role in IT system security and to help foster an understanding of how NSU security policies protect the University employees, students, systems, and data.

1. NSU employees, who manage, administer, operate, or design IT systems, must receive role-based security training that is commensurate with their role.
2. As necessary, OIT will educate and train all stakeholders and appropriate audiences on the policy's content using virtual or face to face engagements.

B. POLICY COMPLIANCE AND VIOLATIONS

1. OIT measures compliance with information security policies and standards through processes that include, but are not limited to monitoring and audits.
2. Violations of this policy will be addressed in accordance with relevant NSU and Commonwealth of Virginia policies, including NSU Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual basis by the appropriate executive or designee.

PUBLICATION

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

- Communicate the policy in writing, electronic or otherwise, to the NSU community within 14 days of approval;
- Submit the policy for inclusion in the online Policy Library within 14 days of approval;

- 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: December 2023
- Approval by, date: December 11, 2020
- Revision History: *New Policy*
- Supersedes policies: *New Policy*

RELATED DOCUMENTS

1. Administrative Policy # 32- 01 (2014) Acceptable Use of Technological Resources: https://www.nsu.edu/policy/admin-32-01.aspx.

2. ITRM Information Security Policy (SEC519): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

3. ITRM Information Security Standard (SEC501): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

4. ITRM Information Security Standard (SEC514): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

5. Virginia Department of Human Resources Management Policy 1.75: http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf?sfvrsn=2