UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38 (2020) System Maintenance Policy

Policy Title:	System Maintenance Policy
Policy Type:	Board of Visitors
Policy Number:	Board of Visitors #38 (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 purpose of the System Maintenance policy is to address the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with the responsibility to implement mobile device access controls. This policy addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any NSU employee or non-NSU representative.

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 8.9 System Maintenance Family, Controls MA-1, MA-2, and MA-5, to include specific requirements for the Commonwealth of Virginia.

TABLE OF CONTENTS PAGE NUMBER

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38 (2020) System Maintenance Policy

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.

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.

System Maintenance: The modification of a system to correct faults, to improve performance, or to adapt the system to a changed environment or changed requirements.

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.

SYSTEM MAINTENANCE POLICY

OIT will develop, disseminate, and review and update the System Maintenance Policy on an annual basis to preserve the confidentiality, integrity, and availability of NSU's information systems, in accordance with SEC501, MA-1, MA-2, and MA-5.

A. CONTROLLED MAINTENANCE

1. The System Owner or designee shall:

   a. Schedule, perform, document, and review records of maintenance and repairs on information system components (including applications, printers, copiers, and scanners) in accordance with manufacturer or vendor specifications and NSU requirements.

   b. Control all maintenance activities, whether performed on-site or remotely and whether the technology is serviced on-site or removed to another location.

   c. Explicitly approve the removal of the information system or system components from NSU facilities for off-site maintenance or repairs.

   d. Sanitize technology to remove all information from associated media before removal from NSU facilities for off-site maintenance or repairs.

   e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair action.

   f. Maintain information system maintenance records for the life of the system that includes:
      - Date and time of maintenance
      - Name(s) of the individual(s) performing the maintenance
      - Name of escort (if necessary)
      - Description of maintenance performed
      - List of technology removed or replaced (including identification numbers if applicable)

B. MAINTENANCE PERSONNEL

1. The System Owner or designee shall ensure that personnel performing maintenance on the information system have required access authorizations or designate NSU personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel does not possess the required access authorizations.

   a. Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, NSU may issue temporary credentials to these individuals.

b. Third-party maintenance providers under contract to perform maintenance/support services on NSU information systems shall provide a list of field service engineers assigned to support maintenance contracts with the following information for each service representative:
   - Name
   - Company represented
   - Title
   - Contact Info (phone number; e-mail)
   - Photo for identification purposes
   - List of systems on which an individual is authorized to perform maintenance

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.

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38 (2020) System Maintenance Policy

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