INFORMATION SECURITY POLICY

Policy Title: Information Security Policy
Policy Type: BOV
Policy Number: 38-10
Approval Date: 10/24/2024
Responsible Office: Office of Information Technology
Responsible Executive: Vice President for Operations and Chief Strategist for Institutional Effectiveness

Applies to: All employees, students, visitors, and contractors, in all academic and operational departments and offices at all Norfolk State University locations, and to all University information technology and data, whether owned and operated by the University, or used for University business through contractual arrangements.

POLICY STATEMENT

All individuals to whom this policy applies shall comply with the Norfolk State University Information Security Standards and protect all IT systems and data to which they have access commensurate with sensitivity and risk. All University information technology and data whether owned and operated by the University, or used for University business through contractual arrangements shall be managed and protected in accordance with the provisions of the Norfolk State University Information Security Standards.

TABLE OF CONTENTS **PAGE NUMBER**

DEFINITIONS

Authorization: The process of verifying that a requested action or service is approved for a specific entity.

Authorize: A decision to grant access, typically automated by evaluating a subject's attributes.

Authorized: A system entity or actor that has been granted the right, permission, or capability to access a system resource.

Availability: The property that data or information is accessible and usable upon demand by an authorized person and that timely, reliable access to data and information services is provided for authorized users.

Computer Network: Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Confidentiality: Protection of systems and data so that unauthorized parties cannot view the data, the property that sensitive information is not disclosed to unauthorized entities, and the assurance that information is not disclosed to unauthorized individuals or processes.

Controlled Unclassified Information (CUI): Information the Federal government owns or has created that needs to be safeguarded and disseminated using only controls consistent with Federal laws, regulations and policies.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems. A Data Custodian may not be a Data Owner or System Owner. A Data Custodian may hold the role of System Administrator.

Data Owner: An individual, who defines, manages, and controls the use of data and ensures compliance with the Information Security Standards with respect to the data. Data Owner may not be a System Administrator.

Information Security: The policies, standards, guidelines, processes, activities, and actions taken to protect the confidentiality, integrity, and availability of information systems and the data they handle commensurate with sensitivity and risk.

Information Security Incident: means an adverse event or situation, whether intentional or accidental, that poses an enterprise impact or threat to the integrity, availability, or confidentiality of University data or systems or requires reporting based upon regulatory requirements.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control.

Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Intellectual Property: Please refer to the BOV POLICY # 35 (2019) INTELLECTUAL PROPERTY POLICY.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

Sensitive Information/Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

System Administrator: An individual or entity that implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian. A System Administrator may not be a Data Owner or System Owner. A System Administrator may also hold the role of Data Custodian.

System Owner: An individual or entity responsible for the operation and maintenance of an IT system. A System Owner may not be a System Administrator.

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the University which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, and computer furnishings operated or maintained by NSU.

Users: Faculty, staff and students as well as others who have been authorized to use Norfolk State University's technological resources, (e.g., contractors, interns, volunteers, etc.).

CONTACT(S)

The Office of Information Technology officially interprets this policy. Questions regarding this policy should be directed to the Office of Information Technology (OIT).

STAKEHOLDER(S)

University Faculty & Staff
Students
Others who have been authorized to use Norfolk State University's technological resources.

ALIGNMENT WITH EXTERNAL FRAMEWORKS

The University's information security program aligns with the Commonwealth of Virginia Information Technology Resource Management Information Security Standard SEC530 and is tailored to the University's environment and unique needs.

RESPONSIBILITIES

The Vice President for Operations and Chief Strategist is authorized to establish information security controls and requirements for all members of the University community. The Vice President for Operations and Chief Strategist, along with the University **Chief Information Officer** (CIO) and **Chief Information Security Officer** (CISO), are responsible for developing and maintaining the University's information security program.

System owners, data owners, data custodians, and system administrators must comply with the Norfolk State University Information Security Policy and Standards and are responsible for assessing the sensitivity for the systems and data for which they are responsible, classifying the systems and data appropriately, implementing controls commensurate with sensitivity and risk, and re-evaluating the systems and data periodically.

All users of University IT resources are required to promptly report information security incidents to the University's Office of Information Technology (OIT) Security Office or OIT Client Services.

In responding to any information security incidents, individuals or departments may not release University information, electronic devices or electronic media to any outside entity, including law enforcement organizations, before notifying the OIT Security Office or OIT Client Services.

The **Chief Information Security Officer** (CISO) is responsible for responding to information security incidents. In addition to following up on reported incidents, the CISO may monitor IT resources for potentially malicious and/or harmful activity and take action deemed necessary based on detected activity, or to enforce a University policy.

SENSITIVE IT SYSTEM ASSESSMENT AND AUDIT

For each IT system owned by Norfolk State University that handles data classified as sensitive, the System Owner and Data Owner(s) shall collaborate with the Office of Information Technology to assess risks to the system and the data it handles as needed, but not less than once every three years.

For each IT system owned by Norfolk State University that handles data classified as sensitive, the System Owner and Data Owner(s) shall cooperate with Internal Audit to conduct an audit of the presence and effectiveness of the controls in the control profile selected for the IT system not less than once every three years for each system.

INFORMATION SYSTEM CONTROL SELECTION AND IMPLEMENTATION

Protecting Norfolk State University's IT systems and data in a manner commensurate with sensitivity and risk in accordance with this Policy requires the selection and implementation of controls that achieve this objective. Accordingly, the System Owner and Data Owner of each IT system owned by Norfolk State University shall collaborate to select and implement information system controls for the IT system and the data it handles that align with the classification of the data the IT system handles under the NSU Data Classification Policy (32-

02) and the risks to which the data are subject.

- **GUIDANCE**
  In most cases, the System Owner and Data Owner will implement controls as defined in the standards documents below based on the Commonwealth's SEC530 Information Security Standard control baselines**https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final**. The control baseline for each IT system should be selected as follows:

Subject system data are classified	Appropriate NIST SP 800-53B profile
Public	Low
Internal	Moderate
Confidential	High
Sensitive	High[1]

Departures from this guidance should be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Information Officer, and the Chief Information Security Officer.

COV SEC530 control families are described below, from which the System Owner and Data Owner should select and implement controls in accordance with the appropriate classification within the NSU Data Classification Policy (32-02).

ACCESS CONTROL (AC)

NSU System and Data Owners must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

AWARENESS AND TRAINING (AT)

NSU System and Data Owners must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of institution information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

AUDIT AND ACCOUNTABILITY (AU)

NSU System and Data Owners must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

[1] In the case of Sensitive systems, the System Owner and Data Owner should consider also implementing control enhancements as outlined in SEC530 Security Standard as appropriate to protect the data.

ASSESSMENT AND AUTHORIZATION (CA)

NSU System and Data Owners must: (i) periodically assess the security controls in institution information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in institution information systems; (iii) authorize the operation of the institution's information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CONFIGURATION MANAGEMENT (CM)

NSU System and Data Owners must: (i) establish and maintain baseline configurations and inventories of institution information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in institution information systems.

CONTINGENCY PLANNING (CP)

NSU System and Data Owners must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the institution's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

IDENTIFICATION AND AUTHENTICATION (IA)

NSU System and Data Owners must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to NSU information systems.

INCIDENT RESPONSE (IR)

NSU System and Data Owners must: (i) establish an operational incident handling capability for institution information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate institution officials and/or authorities.

MAINTENANCE (MA)

NSU System and Data Owners must: (i) perform periodic and timely maintenance on institution information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

MEDIA PROTECTION (MP)

NSU System and Data Owners must: (i) protect information system media, both paper and digital; (ii) limit access to data on information system media to authorized users; and (iii)

employ encryption, where applicable, (iv) sanitize or destroy information system media before disposal or release for reuse.

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

NSU System and Data Owners must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

PLANNING (PL)

NSU System and Data Owners must develop, document, periodically update and implement security plans for institution information systems that describe the security controls in place or planned for the information systems as well as rules of behavior for individuals accessing the information systems.

PROGRAM MANAGEMENT (PM)

NSU must appoint a senior agency Chief Information Security Officer to develop and update the University's information security program plan. The plan documents implementation details about program management and common controls distinct from common, system-specific, and hybrid controls. Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the University.

PERSONNEL SECURITY (PS)

NSU System and Data Owners must: (i) ensure that individuals occupying positions of responsibility within the institution are trustworthy and meet established security criteria for those positions; (ii) ensure that institution information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with NSU security policies and procedures.

RISK ASSESSMENT (RA)

NSU System and Data Owners must periodically assess the risk to institution operations (including mission, functions, image, or reputation), institution assets, and individuals, resulting from the operation of institution information systems and the associated processing, storage, or transmission of institution information.

SYSTEM AND SERVICES ACQUISITION (SA)

NSU System and Data Owners must: (i) allocate sufficient resources to adequately protect institution information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation

restrictions; and (iv) ensure that third-party providers employ adequate security measures, through federal and state law and contract, to protect information, applications and/or services outsourced from the institution.

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

NSU System and Data Owners must: (i) monitor, control and protect institution communications (i.e., information transmitted or received by institution information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within institution information systems.

SYSTEM AND INFORMATION INTEGRITY (SI)

NSU System and Data Owners must: (I) identify, report and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within institution information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

EDUCATION AND COMPLIANCE

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:

- Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
- Submit the policy for inclusion in the online Policy Library within 14 days of approval;
- Post the policy on the appropriate Website; and
- 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.

The Chief Information Security Officer (or designee) 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 Chief Information Security Officer reserves the right to revise or eliminate this policy.

Violations of this policy, including without limitation any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to comply with requirements of this policy may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may violate federal, state, or local laws.

EXCEPTIONS

Exceptions to this policy must be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Information Officer, and the Chief Information Security Officer.

REVIEW SCHEDULE

- Next Scheduled Review:
- Approval by, date:
- Revision History:
- Supersedes (previous policy):

RELATED DOCUMENTS

BOV POLICY # 35 (2019) INTELLECTUAL PROPERTY POLICY
https://www.nsu.edu/policy/bov-35.aspx

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx

32-02 - Data Classification Policy
https://www.nsu.edu/policy/admin-32-02.aspx

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

Codes of Virginia §2.2-2827
https://law.lis.virginia.gov/vacode/title2.2/chapter28/section2.2-2827/