ROLES AND RESPONSIBILITIES STANDARD

Standard Title:	**ROLES AND RESPONSIBILITIES STANDARD (NSU-RR)**
Standard Number:	**38-10.0**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**INFO SECURITY ROLES AND RESPONSIBILITIES**
Approval Date:	**8/16/2024**
Responsible Office:	**Office of Information Technology**
Responsible Executive:	**Chief Information Officer**

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.

STANDARD STATEMENT

All individuals to whom this standard 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.

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.

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.

System Owner: An individual or entity responsible for the operation and maintenance of an IT system.

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 (OIT) officially interprets this standard. OIT is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Questions regarding this standard should be directed to OIT Security.

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

ROLES AND RESPONSIBILITIES (NSU-RR)
PURPOSE
This standard defines the key IT security roles and responsibilities included in the University's Information Security Program. These roles and responsibilities are assigned to individuals and may differ from the role or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

AGENCY HEAD

Each Agency Head is responsible for the security of the agency's IT systems and data. The Agency Head's IT security responsibilities include the following:

a. Designate a Chief Information Security Officer (CISO). The CISO shall report to the Agency Head or designee and is responsible for developing and managing the information security program.

b. Ensure that an agency information security program is maintained, that is sufficient to protect the agency's IT systems, and that is documented and effectively communicated.

c. Review and approve or have the designated CISO review and approve the agency's Business Impact Analyses (BIAs), Risk Assessments (RAs), and Continuity Plan (also referred to as Continuity of Operations Plan or COOP), to include an IT Disaster Recovery Plan, if applicable.

d. Review or have the designated CISO review the System Security Plans for all IT systems classified as sensitive, and:

- Approve System Security Plans that provide adequate protections against security risks; or
- Disapprove System Security Plans that do not provide adequate protections against security risks and require that the System Owner implement additional security controls on the IT system to provide adequate protections against security risks.

e. Ensure internal audit compliance. This compliance must include, but is not limited to:

1. Requiring development and implementation of an audit plan for auditing of

systems classified as sensitive;

2. Requiring that the planned IT security audits are conducted;
3. Receiving reports of the results of IT security audits; and
4. Requiring development of Corrective Action Plans to address findings of IT security audits.

f. Ensure a program of information security safeguards is established.

g. Ensure an information security awareness and training program is established.

h. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

i. Identify a System Owner who is generally the Business Owner for each agency sensitive system. Each System Owner shall assign a Data Owner(s), Data Custodian(s) and System Administrator(s) for each agency sensitive IT system.

j. Prevent or have designee prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:

1. The CISO is not a System Owner or a Data Owner except in the case of compliance systems for information security;
2. The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and
3. The CISO, System Owners, and Data Owners are University employees.

Notes:

- Other roles may be assigned to contractors. For roles assigned to contractors, the contract language must include specific responsibility and background check requirements.
- A System Owner can own multiple IT systems.
- A Data Owner can own data on multiple IT systems.
- System Administrators can assume responsibility for multiple IT systems.

CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO is responsible for development and coordination of the University Information Security Program and, as such, performs the following duties:

a. Administers the University's Information Security Program and periodically assesses whether the program is implemented in accordance with University Information Security Policies and Standards.

b. Reviews requested exceptions to Information Security Policies, Standards and Procedures.

c. Provides solutions, guidance, and expertise in IT security.

d. Maintains awareness of the security status of sensitive IT systems.

e. Facilitates effective implementation of the Information Security Program, by:

1. Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;

2. Collecting data relative to the state of IT security and communicating as needed;

3. Providing consultation on balancing an effective information security program with business needs.

f. Verify and validate that all agency IT systems and data are classified for sensitivity.

g. Develop and maintain an information security awareness and training program for agency staff, including contractors and IT service providers. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually, thereafter.

h. Implement and maintain the appropriate balance of preventative, detective and corrective controls for agency IT systems commensurate with data sensitivity, risk and systems criticality.

i. Mitigate and report all IT security incidents in accordance with §2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence.

j. Maintain liaison with the COV CISO.

PRIVACY OFFICER

An agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA). Otherwise, these responsibilities are carried out by the CISO. The Privacy Officer provides guidance on:

a. The requirements of state and federal Privacy laws.

b. Disclosure of and access to sensitive data.

c. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

SYSTEM OWNER

The System Owner is the agency business manager responsible for having an IT system operated and maintained. With respect to IT security, the System Owner's responsibilities include the following:

a. Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.

b. Managing system risk and developing any additional information security policies and

procedures required to protect the system in a manner commensurate with risk.

c. Maintain compliance with University Information Security policies and standards in all IT system activities.

d. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

e. Designate System Administrators for the system.

DATA OWNER

The Data Owner is the manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

a. Evaluate and classify sensitivity of the data.

b. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

c. Communicate data protection requirements to the System Owner.

d. Define requirements for access to the data.

Note: The Data Owner must enforce all controls and processes required to protect all data classified as sensitive from compromise, unauthorized alteration, or loss. Therefore, the Data Owner is responsible for the protection of all data classified as sensitive regardless of the actions of any assigned data custodian and must ensure that each data custodian allowed access to the sensitive data has the knowledge and capabilities required to protect the confidentiality, integrity, and availability of the data.

SYSTEM ADMINISTRATOR

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists agency management in the day-to-day administration of agency IT systems and implements security controls and other requirements of the agency information security program on IT systems for which the System Administrator has been assigned responsibility.

DATA CUSTODIAN

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

a. Protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

b. Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.

c. Providing Data Owners with reports, when necessary and applicable.

IT SYSTEM USERS

All users of COV IT systems including, but not limited to, employees and contractors are responsible for the following:

a. Reading and complying with agency information security program requirements.

b. Reporting breaches of IT security, actual or suspected, to their the CISO or designee.

c. Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.

EDUCATION AND COMPLIANCE

This standard 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 standard in writing, electronic or otherwise, to the University community within 30 days of approval;
- Post the standard on the appropriate website; and
- Educate and train all stakeholders and appropriate audiences on the standard's content, as necessary. Failure to meet the publication requirements does not invalidate this standard.

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

Violations of this standard, 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 standard 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 standard 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: 8/16/2025
- Approval by, date: OIT CISO, 8/16/2024
- Revision History: N/A

- Supersedes: SEC530 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

RELATED DOCUMENTS

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
38-10 - Information Security Policy