**UNIVERSITY INFORMATION SECURITY POLICY (UISP)**
**BOV #38-03 (2021) System and Services Acquisition Policy**

| | |
|---|---|
| **Policy Title**: | System and Services Acquisition Policy |
| **Policy Type**: | Board of Visitors |
| **Policy Number**: | BOV #38-03 (2021) |
| **Approval Date**: | May 14, 2021 |
| **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 System and Services Acquisition policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of system and services acquisition controls at Norfolk State University. This includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, system and services acquisition best practices, and the requirements defined in this policy. An emphasis on trustworthy systems and supply chain is necessary to achieve a consistent security posture across NSU.

This policy also meets the control requirements outlined in Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC501, Section 8.15 System and Services Acquisition Family, Controls SA-1, SA-2, SA-3, SA-3-COV-1, SA-3-COV-2, SA-6-COV, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SA-22.

**Table of Contents** **Page Number**

## DEFINITIONS

**Authentication**: The process of verifying an identity of a user to determine the right to access specific types of data or IT system.

**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.

**Enterprise Cloud Oversight Services (ECOS)**: Provides oversight functions and management of cloud-based services, specifically focused on Software-as-a-Service (SaaS). ECOS assures compliance and improved security by providing transparency via oversight.

**Encryption**: The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users.

**Fuzz Testing**: This is a software testing technique that provides random data ("fuzz") to the inputs of a program. If the program fails (for example, by crashing, or by failing built-in code assertions), the defects can be noted.

**Information Security Officer (ISO)**: The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's information security program.

**Information Technology (IT)**: 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, data files and/or documents managed or maintained by the University which reside on disk, tape or other media.

**Input Validation**: Checking the type and content of data supplied by a user or application (i.e., input validation, for web applications, means verifying user inputs provided in web forms, query parameters, and uploads).

**Least Privilege**: The minimum level of data, functions, and capabilities necessary to perform a user's duties.

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

**Penetration Testing**: A penetration test is a method of evaluating the security computer system or network simulating an attack by a malicious user.

**Project Definition**: The process of identifying the specific schedule activities that need to be performed to produce the various project deliverables.

**Project Disposition**: This is the end of a system's life cycle. The system is retired according to organizational needs, laws and regulations. Disposition activities ensure that the system is terminated in an orderly manner and that vital information about the system is preserved for future access.

**Project Implementation**: This occurs when products that have completed testing are moved into production or into their working environment.

**Project Initiation**: This is the start of the project, and the goal of this phase is to define the project at a broad level. This phase usually begins with a business case.

**Quality Assurance**: The process of evaluating overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards.

**Risk Assessment**: The process of identifying and evaluating risks so as to assess their potential impact. A review, examination, and judgment of whether or not the identified risks are acceptable.

**Sensitive 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.

**Session Management**: The process of securely handling multiple requests to an application or service from a single user or entity. It is a series of requests and response transactions created by the same user.

**System Development Life Cycle Methodology**: A project management model that defines the stages involved in bringing a project from inception to completion.

**System Security Plan**: An overview of the security requirements of a system. It describes the controls in place or planned, responsibilities, and expected behavior of all individuals who access the system.

## CONTACT(S)

The Office of Information Technology (OIT) 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 AND SERVICES ACQUISITION POLICY

OIT will review and update the System and Services Acquisition policy on an annual basis or more frequently if required to address changes.

### A. ALLOCATION OF RESOURCES

1. The CIO or designee shall:

    a. Determine IT security requirements for systems or services in mission/business process planning.

        i. IT security priorities and requirements at the project and enterprise level must be integrated into business cases.

        ii. Business case analysis must consider how to employ and leverage existing NSU components before new technology investments may be proposed.

    b. Determine, document, and allocate the resources required to protect systems or services as part of the University's capital planning and investment control process.

### B. LIFE CYCLE SUPPORT

1. The ISO or designee shall:

    a. Manage systems by using a system development life cycle methodology that incorporates security considerations.

    b. Define and document security roles and responsibilities throughout the system development life cycle.

    c. Identify individuals having IT security roles and responsibilities.

d. Integrate the University's IT security risk management process into system development life cycle activities.

2. The ISO or designee conducts:

   a. Project Initiation

      i. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level IT security guidelines for system developers.

      ii. Classify the types of data that the IT system will process and the sensitivity of the proposed IT system.

      iii. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.

      iv. Develop an initial IT System Security Plan that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.

   b. Project Definition

      i. Identify, develop, and document IT security requirements for the IT system.

      ii. Incorporate IT security requirements in IT system design specifications.

      iii. Verify that the IT system development process designs, develops, and implements IT security controls that meet IT security requirements in the design specifications.

      iv. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system in order to provide adequate protection against IT security risks.

      v. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.

c. Project Implementation

i. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

ii. Conduct a Risk Assessment to assess the risk level of the IT application system.

iii. Require that the system comply with all relevant Risk Management requirements in Virginia Information Technologies Agency's (VITA's) security standards.

iv. Update the IT System Security Plan to document the implemented IT security controls included in the IT system in order to provide adequate protection against IT security risks, and to comply with other requirements.

d. Project Disposition

i. Require retention of the data handled by an IT system in accordance with the University's records retention policy prior to disposing of the IT system.

ii. Require that electronic media be sanitized prior to disposal so that all data is removed from the IT system.

iii. Verify the disposal of hardware and software in accordance with the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).

3. The ISO or designee shall be accountable for ensuring the following steps are documented and followed:

a. Application Planning

i. Data Classification – Data used, processed, or stored by the proposed application shall be classified according to the sensitivity of the data.

ii. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete.

iii. Security Requirements – Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.

iv. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process, or store sensitive information in an application, the University must address the following design criteria:

1. Encrypted communication channels shall be established for the transmission of sensitive information.

2. Sensitive information shall not be transmitted in plain text between the client and the application.

3. Sensitive information shall not be stored in hidden fields that are part of the application interface.

b. Application Development – require a set of coding practices, which shall be applied to all applications under development, such as:

i. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.

ii. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.

iii. Data storage shall be separated either logically or physically, from the application interface.

iv. NSU shall not use or store sensitive data in non-production environments (i.e., a development or test environment) that does not have security controls equivalent to the production environment.

v. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.

vi. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted.

vii. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.

viii. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.

ix. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.

c. Production and Maintenance

i. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.

ii. Internet-facing applications classified as sensitive shall have periodic, not to exceed 90 days, vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

## C. INFORMATION SYSTEM DOCUMENTATION

1. The ISO or designee shall:

a. Obtain administrator documentation (whether published by a vendor/manufacturer or written in-house) for the IT system, component, or service that describes:

i. Secure configuration, installation, and operation of the system, component, or service.

ii. Effective use and maintenance of security functions/mechanisms.

iii. Known vulnerabilities regarding configuration and use of administrative (privileged) functions.

b. Obtain user documentation (whether published by a vendor/manufacturer or written in-house) for the IT system, component, or service that describes:

i. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.

ii. Methods for user interaction, which enables individuals to use the IT system, component, or service in a more secure manner.

iii. User responsibilities in maintaining the security of the IT system, component, or service.

c. Document attempts to obtain IT system, component, or system service documentation when such documentation is either unavailable or nonexistent and implements the appropriate NSU-defined actions in response.

d. Protect documentation as required, in accordance with the risk management strategy.

e. Distribute documentation to the appropriate NSU-defined personnel.

## D. SOFTWARE USAGE RESTRICTIONS

1. The CIO or designee shall or shall require that service providers document software license management practices that address, at a minimum, the following:

a. Require the use of only NSU approved software and service provider approved systems management software on IT systems.

b. Assess periodically whether all software is used in accordance with license agreements.

## E. SECURITY ENGINEERING PRINCIPLES

1. The DIS or designee shall apply IT system security engineering principles in the specification, design, development, implementation, and modification of the IT system. Security engineering principles include, but are not limited to:

    a. Developing layered protections.

    b. Establishing sound security policy, architecture, and controls as the foundation for design.

    c. Incorporating security into the SDLC.

    d. Delineating physical and logical security boundaries.

    e. Ensuring system developers and integrators are trained on how to develop secure software.

    f. Tailoring security controls to meet organizational and operational needs.

    g. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

    Note: For legacy information systems, security engineering principles must be applied to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

## F. EXTERNAL INFORMATION SYSTEM SERVICES

1. The ISO or designee shall:

    a. Require that providers of external IT system services comply with NSU IT Security requirements and employ appropriate security controls in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance.

    b. Define and document government oversight and user roles and responsibilities with regard to external IT system services.

i. Documents that solicit and implement external information system services must:

1. Identify specific drivers for soliciting the services.

2. Identify associated reporting requirements.

3. Include in the procurement any Service-Level Agreements (SLA's). SLA's must:

i. Define expectations of performance for each required security control.

ii. Describe measurable outcomes.

iii. Specify remedies and response requirements for any identified instance of non-compliance.

c. Employ appropriate processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

i. Where a sufficient level of trust cannot be established with an external service provider, employ compensating security controls or accept the degree of risk.

## G. DEVELOPER CONFIGURATION MANAGEMENT

1. The ISO or designee shall require the developer of the IT system, component, or service to:

a. Perform configuration management during IT system design, development, implementation, and operation.

b. Document, manage, and control the integrity of changes to the configuration items under configuration management.

c. Implement only NSU-approved changes to the system, component, or service.

d. Document approved changes to the system, component, or service and the potential security impacts of such changes.

e. Track security flaws and flaw resolution within the system, component, or service and report findings to the appropriate NSU-defined personnel.

## H. DEVELOPER SECURITY TESTING

1. The DIS or designee shall require developers of IT systems, components, or services to:

    a. Create and implement a security assessment plan.

    b. Perform unit, integration, system, and regression testing/evaluation at the appropriate depth and coverage.

        i. Requirements for testing and retesting (after significant changes) must be included in:

            1. Contractual documents for development and system integration.

            2. Internal development procedures.

    c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation. Evidence must support that:

        i. A control is in place and operating as intended.

        ii. A control is either not in place or not operating as intended.

        iii. Results are current and the most recent.

    d. Implement a verifiable flaw remediation process.

    e. Correct flaws identified during security testing/evaluation.

    f. Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

    g. Perform a manual code review of specific code using the appropriate processes, procedures, and/or techniques.

    h. Perform penetration testing at the appropriate breadth/depth and with documented NSU-defined constraints.

i. Perform attack surface reviews.

j. Verify that the scope of security testing/evaluation provides complete coverage of required security controls at the appropriate depth of testing/evaluation.

## I. DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

1. The DIS or designee shall:

   a. Require developers of IT systems, components, or services to follow a documented development process that:

      i. Explicitly addresses security requirements.

      ii. Identifies the standards and tools used in the development process.

      iii. Documents the specific tool options and tool configurations used in the development process.

      iv. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

   b. Review the development process, standards, tools, and tool options/configurations on an annual basis or more frequently if required to address an environmental change to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy NSU-defined security requirements.

## J. DEVELOPER PROVIDED TRAINING

1. The CIO or designee shall require developers of IT systems, components, or services to provide NSU-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

## K. DEVELOPER SECURITY ARCHITECTURE AND DESIGN

1. The DIS or designee shall require developers of IT systems, components, or services to produce a design specification and security architecture that:

a. Is consistent with and supportive of NSU's security architecture which is established within and is an integrated part of the University's enterprise architecture.

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components.

c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

### L. UNSUPPORTED SYSTEM COMPONENTS

1. The CIO or designee shall:

   a. Replace IT system components when support for the components is no longer available from the developer, vendor, or manufacturer.

   b. Provide justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs.

   c. Provide either in-house support or NSU-defined support from external providers for unsupported IT system components.

## 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 IT 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:

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

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

3. 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: May 2024
- Approval by, date: May 14, 2021
- 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

6. Library of Virginia Personnel Records General Schedule (GS)-103 (Feb 2015): https://www.lva.virginia.gov/agencies/records/sched_state/GS-103.pdf