UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38-06 (2021) Change Management Policy

Policy Title:	Change Management Policy
Policy Type:	Board of Visitors
Policy Number:	BOV #38-06 (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 Change Management policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of change management controls at Norfolk State University. This includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, change management best practices, and the requirements defined in this policy. Standardized change control methods and prompt handling of all system and application changes will minimize the impact of change-related incidents as well as the service quality of day-to-day IT operations of the University.

This policy also meets the control requirements outlined in Commonwealth of Virginia Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC-501, Section 8.5, Configuration Management Family, Controls CM-1 through CM-11.

Table of Contents **Page Number**

DEFINITIONS

Change Advisory Board: Responsible for evaluating and approving or disapproving proposed changes, and for ensuring proper implementation of approved changes.

Change Management: A critical discipline that controls and communicates the changes occurring in the IT environment.

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.

Configuration Baseline: Configuration information formally designated at a specific time during a product's or product component's life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information.

Configuration Item (CI): Aggregation of work products that is designated for change management and treated as a single entity in the change management process. This aggregation consists of all required components: hardware, software, and other items that comprise a baseline.

Configuration Item Attributes: Descriptive characteristics of configuration items (CI), such as a make or model number, version number, supplier, purchase contract number, release number, data format, role or relationship, held in the Configuration Management Database (CMDB).

Configuration Management: A discipline applying technical and administrative direction and surveillance to (1) identify and document the functional and physical characteristics of a configuration item, (2) control changes to those characteristics, (3) record and report change processing and implementation status, and (4) verify compliance with specified requirements.

Configuration Management Database (CMDB): Database that stores attributes of CIs and relationships with other CIs.

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.

Information Technology Assets: NSU's hardware, software, services and applicable documentation.

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

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

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

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

CHANGE MANAGEMENT POLICY

In accordance with SEC501, CM-1 through CM-11 (Configuration Management), OIT will develop, disseminate, and update the Change Management Policy on at least an annual basis. System Owners shall control and document the configuration of information systems and their respective components.

A. BASELINE CONFIGURATION

1. The System Owner or designee shall:

    a. Develop, document, and maintain under change control, a current baseline configuration of the information system including communications and connectivity-related aspects of the system. At a minimum, the baseline configuration shall include:

        i. Standard operating system/installed applications with current version numbers.
        ii. Standard software load for workstations, servers, network components, and mobile devices and laptops.

        iii. Up-to-date patch level information.

        iv. Network topology.

        v. Logical placement of the component within the system and enterprise architecture.

        vi. Technology platform.

b. Maintain the baseline configuration of the information system to be consistent with OIT's enterprise architecture.

c. Develop and maintain an organization-defined list of software programs authorized to execute on the information system.

d. Employ a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

e. Maintain a baseline configuration for development and test environments that are managed separately from the operational baseline configuration.

f. Identify, document, and apply more restrictive security configurations for sensitive IT systems, as necessary.

g. Maintain records that document the application of baseline security configurations.

h. Monitor systems for security baselines and policy compliance.

i. Reapply all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.

j. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

k. Periodically review a list of hardware IT assets.

l. Create and periodically review a list of software assets.

m. Review and update the baseline configuration of the information system:

    i. Once a year at a minimum.

    ii. When required due to a significant configuration change, such as an operating system upgrade or hardware change, or a demonstrated vulnerability.

    iii. As an integral part of information system component installations and upgrades.

2. Require the following additional configuration changes to devices to be used for international travel:

i. Install all operating system security updates.

ii. Install all anti-virus, firewall, and anti-spyware security application software updates.

iii. Encrypt the computer hard disk or at least all sensitive information on the device.

iv. Update the web browser software and implement strict security settings.

v. Update all application software to be used during the trip.

vi. Disable infrared ports, Bluetooth ports, web cameras, and any hardware features not needed for the trip.

vii. Configure the device to use a VPN connection to create a more secure connection.

viii. Configure the device to disable sharing of all file and print services.

ix. Configure the device to disable ad-hoc wireless connections.

x. Ensure that all required cables and power adapters are packed with the computing asset.

B. CHANGE CONTROL

1. System Owner and Administrator shall be responsible for the following:

   a. Determine the types of changes to the information system that are configuration controlled.

   b. Approve configuration-controlled changes to the system with explicit consideration for security impact analyses.

   c. Document approved configuration-controlled changes to the system.

   d. Retain and review records of configuration-controlled changes to the system.

   e. Audit activities associated with configuration-controlled changes to the system. Audit of changes must include changes in activity before and after changes are made to the information system and the auditing activities required to implement the change.

f. Coordination and oversight for configuration change control activities through a Change Advisory Board (CAB) that convenes on a bi-weekly basis to review changes prior to implementation.

g. Test, validate, and document changes to the information system before implementing the changes on the operational system.

h. Ensure the individual or group-conducting tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process.

i. Acknowledgment that an operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible.

j. Warrant, in situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

k. Ensure configuration change control for the information system shall involve the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications.

l. Ensure configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, and routers), emergency changes, and changes to remediate flaws.

m. Ensure processes and procedures are in place to effectively manage cryptographic mechanisms used to provide system security safeguards.

n. Ensure all changes to IT assets used by NSU shall be made in accordance with best practices where it does not conflict with NSU's mission.

o. Confirm service providers make all changes to IT assets that it supplies for use by NSU in accordance with best practices, where it does not conflict with NSU's mission.

p. Require that service providers document, implement configuration management, and change control practices so that changes to the IT environment do not compromise security controls.

C. SECURITY IMPACT ANALYSIS

1. The DIS or designee shall analyze changes to the information system to determine potential security impacts prior to change implementation.

    a. Individuals conducting security impact analyses must have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

    b. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls.

    c. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required.

    d. Security impact analysis is scaled in accordance with the security categorization of the information system.

    e. An information security representative shall be a member of the CAB.

D. ACCESS RESTRICTIONS FOR CHANGE

1. The System Owner shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

    a. Ensure only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

        i. Ensure no local administrative rights will be granted without the submission of an Administrative/Root Access Request Form and approval of DIS or designee.

        ii. Maintain records of access. Access records are essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system.

iii. Ensure logical and physical access control lists that authorize qualified individuals to make changes to an information system or component is created and maintained.

b. Access restrictions for change also include software libraries. The System Owner shall:

i. Limit information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment.

ii. Review and reevaluate information system developer/integrator privileges annually.

E. CONFIGURATION SETTINGS

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections.

1. The System Owner or designee shall:

a. Establish and document mandatory configuration settings for information technology products employed within the information system using appropriate standards that reflect the most restrictive mode consistent with operational requirements.

i. A standard set of mandatory configuration settings must be established and documented for information technology products employed within the information system.

b. Implement the configuration settings.

c. Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements.

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

F. LEAST FUNCTIONALITY

1. The DIS or designee shall verify that the information system is configured to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services that are not required for the business function of the information system.

    a. The System Owner has developed system-hardening baselines for the operating systems known to be in use within NSU. OIT will also utilize the system hardening baselines established by The Center for Internet Security (CIS) for those systems not addressed by the NSU-specific system hardening baselines.

    b. In cases where a baseline security configuration does not exist for an operating system, the DIS or designee shall ensure a baseline security configuration is developed, documented and approved.

    c. Relevant staff shall apply these baseline security configurations to all operating systems. Where NSU and Center for Internet Security (CIS) benchmarks document Level 1 and Level 2 baseline security configurations, unless otherwise approved by the DIS or designee, NSU shall use:

        i. Level 1 configurations for internal IT systems.

            a. The Level 1 is a baseline security recommendation that can be implemented promptly and is designed not to have an extensive performance impact. The intent of the Level 1 is to lower the attack surface of NSU while keeping machines usable and not hindering business functionality.

        ii. Level 2 configurations for internet- and/or customer-facing IT systems.

            a. The Level 2 is considered "defense in depth" baseline and is intended for environments where security is paramount. The recommendations associated with the Level 2 baseline can have an adverse effect on NSU if not implemented appropriately or without due care.

    d. Any exceptions to baseline security configurations must be documented by security operations staff in writing and approved by the DIS or designee.

    e. System Owner shall require that relevant staff maintain records confirming the implementation of baseline security configurations for each IT system they manage.

f. System Owner shall require that baseline security implementation records be audited annually by the DIS or designee to verify the implementation of the appropriate baseline security configurations.

g. System Owners shall require that security operations staff perform network vulnerability scans of all server and NSU administrative desktop computers on a frequency consistent with best practices and state policy.

h. The DIS or designee shall review the results of the IT system vulnerability scans when completed.

i. System Owner shall require that sensitive internal-facing web applications be scanned for vulnerabilities on an annual basis. Sensitive external-facing web applications must be scanned for vulnerabilities on a quarterly basis. This scanning may be performed by security operations staff, system owners or Commonwealth Security and Risk Management staff as is appropriate and convenient.

j. All identified operating system and application vulnerabilities will be remediated without undue delay according to the severity and risk utilizing NSU's Change Management Policy and procedure.

k. Ensure where feasible, the organization will limit component functionality to a single function per device (e.g., email server or web server, not both).

G. INFORMATION SYSTEM COMPONENT INVENTORY

1. The System Owner shall develop, document, and maintain an inventory of information system components that:

   a. Accurately reflects the current information system.

   b. Is consistent with the authorization boundary of the information system.

      i. All components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

   c. Is at the level of granularity deemed necessary for tracking and reporting.

   d. Includes organization-defined information deemed necessary to achieve effective property accountability, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license

information, information system/component owner, and for a networked component/device, the machine name and network address.

i. The updated system and network diagrams must be maintained.

e. Is available for review and audit by designated organizational officials.

f. Is updated as an integral part of component installations, removals, and information system updates.

g. Is included in property accountability information, a means for identifying by name, position, or role, individuals responsible for administering those components.

i. A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

h. Includes assessed component configurations and any approved deviations to currently deployed configurations in the information system component inventory.

2. The inventory of information system components must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:

a. Manufacturer

b. Type

c. Model

d. Serial number

e. Physical location

f. Software license information

g. Information system/component owner

h. Associated component configuration standard

i. Software/firmware version information

j. Networked component/device machine name or network address

k. Ownership

Note: Data and homogeneous systems, belonging to NSU, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

Note: Where more than one department may own the IT system, and the department or departments cannot reach a consensus on which should serve as System Owner for the purposes of this Standard, upon request, the CIO will determine the System Owner.

H. CHANGE MANAGEMENT PLAN

1. The DIS or designee shall develop, document, and implement a change management plan for the information system that:

    a. Addresses roles, responsibilities, and change management processes and procedures.

    b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under change management.

    c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

    d. Assigns responsibility for developing the change management process to organizational personnel that are not directly involved in system development.

        i. In the absence of a dedicated change management team, the system integrator may be tasked with developing the change management process.

    e. Defines detailed processes and procedures for how change management is used to support system development life cycle activities at the information system level.

    f. Describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated.

2. The change management approval process must include:

a. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system.

b. Designation of personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

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:

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