Christopher Newport University

Policy: Information Technology Change Management Policy
Policy Number: 6035

Executive Oversight:	Vice President for Finance and Planning/CFO
Contact Office:	Information Technology Services
Frequency of Review:	Annually
Date of Last Review:	January 2022

A. PURPOSE

This policy defines the standards of practice for implementation, modification, and maintenance of production hardware, software, and information systems and serves to establish and maintain the integrity of Christopher Newport University's production technology systems. It also satisfies the Commonwealth's configuration management and change control requirements defined in VITA SEC 501-10.

B. POLICY STATEMENT

The University shall provide and implement technology-related changes in a manner that provides flexibility, manages risk, and maintains transparency.

C. PROCEDURES

All campus System Owners, Systems Administrators, Data Custodians, and Data Owners shall take steps to adopt and implement change management procedures that:

- Track requests and approvals;
- Track the development and change process;
- Document evidence of testing and end-user validation (or lack of testing);
- Document privacy and security considerations relative to the change;
- Document potential risk to the University if change fails or does not occur;
- Document production deployments, including communication planning;
- Provide historical tracking for all requested changes whether implemented or withdrawn; and
- Aid recovery and rollback efforts, by tracking specific changes to code and configuration.

The Change Management Board (CMB) shall define and maintain configuration and change management for the University's production hardware and software infrastructure. Changes to systems that house or collect sensitive data shall be reported to the CMB.

The change management process shall accommodate urgent changes, standard changes, and routinely occurring preapproved changes.

The specific Information Technology Services (ITS) change process shall be available on the ITS internal website.

D. DEFINITIONS

Change: Modifications of the current state of a technology-related application, process, or service, which could impact end-user functionality or pose a significant risk to University production technology systems.

Examples include:

- New system implementations and the launch of new applications that may store or interact with university data
- Application modifications or updates such as a Banner upgrade or new system implementation
- Hardware modifications or updates such as data storage system upgrade
- Software modifications or updates such as an HRIS feature update or implementation
- Network modifications or updates such as a University firewall upgrade or implementation
- Process modifications or updates such as VPN approval process updates

Data entry and regularly occurring low-risk operational changes are not considered changes subject to this policy.

Change Management Board: Committee established by Information Technology Services (ITS) that convenes on a regular basis to make recommendations regarding whether or not proposed technology-related changes should be implemented. As required by SEC 501.10 CM-3, the University Information Security Officer (ISO) serves on the committee.

Change Request: A record of a given change, which includes consideration of risk, university schedule, communication, and status (withdrawn/complete).

Data Custodian: An individual authorized by the Data Owner to be in physical or logical possession of data. The Data Custodian is responsible for the protection of data from unauthorized access, alteration, destruction or usage. The Data Custodian may also be a System Administrator.

Data Owner: The manager responsible for policy and practice decisions regarding the evaluation and classification of data sensitivity, definition and communication of data protection requirements to the System Owner, and definition of requirements for access to the data.

Hardware, software, and information systems: University technology-related assets which work together or independently to provide a service to the University.

Production Systems: Systems critical to the operation of a specific department or the University.

Significant Risk: A risk that poses operational concern for a majority of the University, or might impair the operation of an entire department.

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

System Owner: The manager responsible for the operation and maintenance of an IT system. IT systems may have only one System Owner. The System Owner manages system risk and develops security policies and procedures to protect the system in a manner commensurate with risk; maintains compliance with COV Information Security policies and standards; maintains compliance with requirements specified by Data Owners for the handling of data processed by the system; and designates a System Administrator for the system.

E. REFERENCES

VITA SEC 501- IT Information Security Standard

VITA SEC 501 CM-1 – Configuration Management Policies and Procedures

VITA SEC 501 CM-3-COV – Configuration Change Control

VITA SEC 501 CM-4-COV – Security Impact Analysis

VITA SEC 501 CM-5 – Access Restrictions for Change

F. APPROVAL AND REVISIONS

Approved By: Policy Committee, February 20, 2019
Revision 1: Policy Committee, October 5, 2020
Revision 2: Policy Committee, January 12, 2022

G. NEXT REVIEW DATE: Spring 2023