



OIT 62.1004: Configuration Management and Change Control

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

Configuration Management and Change Control concerns protection of the components that comprise IT systems by managing them in a planned, organized, and secure fashion.

II. Purpose

Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes to these items during their life cycles. While the full extent of Configuration Management and Change Control is beyond the scope of this document, NSU should institute structured practices in this area, based on industry standard frameworks such as the IT Infrastructure Library (ITIL) (www.itil.co.uk) or Control Objectives for Information and related Technology (COBIT) (www.isaca.org), among others.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

NSU shall, or shall require that its service provider, document and implement configuration management and change control practices so that changes to the IT environment do not compromise security controls.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the

appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer 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 Information Security Officer reserves the right to revise or eliminate this policy.