Policy Title: Configuration Change Control

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 503 (2014) Configuration Change Control

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

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, routers), emergency changes, and changes to remediate flaws.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CONTACT(S)</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>1</td>
</tr>
<tr>
<td>Stakeholder(s)</td>
<td>2</td>
</tr>
<tr>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>3</td>
</tr>
<tr>
<td>Interpretation</td>
<td>3</td>
</tr>
<tr>
<td>Publication</td>
<td>3</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>4</td>
</tr>
<tr>
<td>Related Documents</td>
<td>4</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869
STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology

PURPOSE

This control is intended to establish the policy and procedures for configuration change control on all University information system components.

REQUIREMENTS

NSU:

1. Determines the types of changes to the information system that are configuration controlled;

2. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;

3. Documents approved configuration-controlled changes to the system;

4. Retains and reviews records of configuration-controlled changes to the system;

5. Audits activities associated with configuration-controlled changes to the system; and

6. Coordinates and provides oversight for configuration change control activities through a Change Control Board that convenes on a regular basis to review changes prior to implementation.

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.

Supplemental Guidance: NSU determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. A typical University process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change.

Control Enhancements for Sensitive Systems:
1. NSU tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Enhancement Supplemental Guidance: NSU ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the University 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. 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. In situations where the University cannot conduct testing of an operational system, the University employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

2. NSU requires an information security representative to be a member of the University-defined configuration change control element (e.g., committee, board).

Enhancement Supplemental Guidance: Information security representatives can include, for example, information system security officers or information system security managers.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 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.

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.

PUBLICATION

This policy 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:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. 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: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:
  - Supersedes (previous policy): OIT 62.8.50.3 Configuration Change Control

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard