Policy Title: Baseline Configuration

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 502 (2014) Baseline Configuration

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the components within the system architecture.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Contacts</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder(s)</td>
<td>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>1</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
PURPOSE

This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system.

REQUIREMENTS

NSU develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

NSU:

1. Identifies, documents, and applies more restrictive security configurations for sensitive agency IT systems, as necessary.

2. Maintains records that document the application of baseline security configurations.

3. Monitors systems for security baselines and policy compliance.

4. Reviews and revises all security configuration standards annually, or more frequently, as needed.

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

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

7. Requires creation and periodic review of a list of agency hardware and software assets.

8. Reviews and updates the baseline configuration of all information system:

   a. Once a year at a minimum;

   b. When required due to a significant configuration change or a demonstrated vulnerability; and

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

Supplemental Guidance: The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating
new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the NSU’s enterprise architecture.

Control Enhancements for Sensitive Systems:

1. NSU develops and maintains a University-defined list of software programs authorized to execute on the information system; and

2. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system; and

3. Maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

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.
ADMINISTRATIVE POLICY # 32 – 8 – 502 (2014) Baseline Configuration

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 62.8.502 Baseline Configuration

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard