Policy Title: Information System Documentation

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1505 (2014) Information System Documentation

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Information system documentation is a critical element of the University’s information system and the security measures implemented for sustained operation of the system. This documentation details configurations, essential components, and other crucial aspects of the information system.

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 the development, maintenance, and regular review of the University’s information system documentation.

REQUIREMENTS

NSU:

1. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
   a. Secure configuration, installation, and operation of the information system;
   b. Effective use and maintenance of security features/functions; and
   c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and

2. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
   a. User-accessible security features/functions and how to effectively use those security features/functions;
   b. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
   c. User responsibilities in maintaining the security of the information and information system; and

3. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Supplemental Guidance: The inability of the University to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, the University may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls. Service providers provide assurance that this control is met where applicable.
Control Enhancements for Sensitive Systems:

1. NSU obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

2. NSU obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.

3. NSU obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.

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 62.8.1505 Information System Documentation

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard