Policy Title: Sensitive IT System Inventory and Definition

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 5 (2014) Sensitive IT System Inventory and Definition

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Sensitive IT System Inventory and Definition addresses protecting University information and IT systems commensurate with sensitivity and risk, including system availability needs. This is a central component of the University information security program and allows the University to determine how these factors apply to its IT systems and data.

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>2</td>
</tr>
<tr>
<td>Interpretation</td>
<td>2</td>
</tr>
<tr>
<td>Publication</td>
<td>3</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>3</td>
</tr>
<tr>
<td>Related Documents</td>
<td>3</td>
</tr>
</tbody>
</table>

CONTACT(S)

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

University Faculty & Staff
Office of Information Technology

PURPOSE

The Sensitive IT System Inventory and Definition policy identifies the steps in listing and marking the boundaries of sensitive IT systems in order to provide cost-effective, risk-based security protection for IT systems, for the University as a whole.

REQUIREMENTS

The ISO or designated Sensitive System Owner(s) shall:

1. Document each sensitive IT system owned by the University, including its ownership and boundaries, and update the documentation as changes occur.

   **Note:** Data and homogenous systems, belonging to the University, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

   **Note:** Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner for the purposes of this Policy, upon request, the CIO of the Commonwealth will determine the System Owner.

   **Note:** A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

2. Maintain or require that its service provider maintain updated network diagrams.

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.

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.
PUBLICAION

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 62.5 Sensitive IT System Inventory and Definition

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard