Policy Title: System Security Plan

Policy Type: Administrative


Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

A system security plan is an integral component for safeguarding the University’s information system from potential threats and mitigating the intrinsic risks associated with hosting services that employ both general and potentially sensitive data.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>1</td>
</tr>
<tr>
<td>Stakeholder(s)</td>
<td>1</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 and regular review of a system security plan for the University’s information system.

REQUIREMENTS

NSU:

1. Develops a security plan for the information system that:
   a. Is consistent with the University’s enterprise architecture;
   b. Explicitly defines the authorization boundary for the system;
   c. Describes the operational context of the information system in terms of missions and business processes;
   d. Provides the security categorization of the information system including supporting rationale;
   e. Describes the operational environment for the information system;
   f. Describes relationships with or connections to other information systems;
   g. Provides an overview of the security requirements for the system;
   h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
   i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

2. Reviews the security plan for the information system every three years, or more often if necessary (i.e. due to material change), and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.; and

3. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

NSU shall:

1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of:
a. All IT existing and planned IT security controls for the IT system, including a schedule for implementing planned controls;

b. How these controls provide adequate mitigation of risks to which the IT system is subject.

2. Submit the IT System Security Plan to the Agency Head or designated ISO for approval.

3. Plan, document, and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

Supplemental Guidance: The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to University operations and assets, individuals, other organizations, and the Commonwealth if the plan is implemented as intended.

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 62.8.1202 System Security Plan

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard