Policy Title: Separation of Duties

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

Separation of duties is a control utilized in order to reduce the possibility of any individual(s) conducting malevolent activity by separating responsibilities amongst multiple roles and/or titles.

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>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>2</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

This control is intended to establish the policy and procedures for implementing separation of duties as it applies to the roles and responsibilities of University personnel.

REQUIREMENTS

NSU:

1. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;

2. Documents separation of duties; and

3. Implements separation of duties through assigned information system access authorizations.

Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles.

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 62.8.105 Separation of Duties

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard