**Policy Title:** Audit and Accountability Policy and Procedures

**Policy Type:** Administrative

**Policy Number:** ADMINISTRATIVE POLICY # 32 – 8 – 301 (2014) Audit and Accountability Policy and Procedures

**Approval Date:** 05/28/2014 Revised

**Responsible Office:** Office of Information Technology

**Responsible Executive:** CIO

**Applies to:** Office of Information Technology

**POLICY STATEMENT**

Auditing and Accountability is required in order to maintain integrity and compliance throughout all OIT departments. The requirements for this family of policies are directly addressed within.

**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>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>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 produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family.

REQUIREMENTS

NSU develops, disseminates, and reviews/updates at least annually:

1. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

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 62.8.301 Audit and Accountability Policy and Procedures

**RELATED DOCUMENTS**

Virginia Commonwealth State policy SEC501-08 Information Security Standard