Policy Title: Auditable Events

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 302 (2014) Auditable Events

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

NSU determines at its discretion, in accordance with applicable Commonwealth laws and regulations, events that can be considered auditable in conjunction with the following requirements.

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>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>3</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

This control is intended to establish the policy and procedures for the determination of events which need to be auditable within the University’s information system.

REQUIREMENTS

NSU:

1. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: authentication attempt, authenticated individual, access time, source of access, duration of access, and actions executed.

2. Coordinates the security audit function with other University entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events; and

3. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

Supplemental Guidance: The purpose of this control is for the NSU to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, NSU may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

Control Enhancements for Sensitive Systems:

1. NSU reviews and updates the list of auditable events at least annually.

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.
ADMINISTRATIVE POLICY # 32 – 8 – 302 (2014) Auditable Events

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 62.8.302 Auditable Events

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard