Policy Title: Audit Review, Analysis, and Reporting

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

Concurrent with Commonwealth polices, audit records are required to be reviewed and analyzed by the appropriate officials within NSU OIT on a predetermined basis so that anomalies that occur or have occurred may be investigated and reported as necessary.

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>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>3</td>
</tr>
<tr>
<td>Related Documents</td>
<td>4</td>
</tr>
</tbody>
</table>
STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology

PURPOSE

This control is intended to establish the policy and procedures for review, analyses and reporting of audits for both general and sensitive components of the University’s information system.

REQUIREMENTS

NSU:

1. Reviews and analyzes information system audit records at least every 30-days for indications of inappropriate or unusual activity, and reports findings to designated NSU officials; and

2. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to University operations, University assets, individuals, other organizations, or the Commonwealth based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements for Sensitive Systems:

1. The information system integrates audit review, analysis, and reporting processes to support University processes for investigation and response to suspicious activities.

2. NSU analyzes and correlates audit records across different repositories to gain University-wide situational awareness.

3. The information system centralizes the review and analysis of audit records from multiple components within the system.

   Enhancement Supplemental Guidance: An example of an automated mechanism for centralized review and analysis is a Security Information Management (SIM) product.

4. NSU integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

   Enhancement Supplemental Guidance: A Security Event/Information Management system tool can facilitate audit record aggregation and consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record
analysis scripts developed by NSU (with localized script adjustments, as necessary), provides a more cost-effective approach for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of the vulnerability scans and correlating attack detection events with scanning results.

**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 62.8.306 Audit Review, Analysis, and Reporting
RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard