Policy Title: Security Awareness

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 202 (2014) Security Awareness

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Information security awareness training is required to provide all IT system users with appropriate understanding regarding University Information Security Policies and acceptable use requirements for IT systems and data.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CONTACT(S)</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Information Technology</td>
<td>(757)823-2869</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STAKEHOLDER(S)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>University Faculty &amp; Staff</td>
<td></td>
</tr>
<tr>
<td>Office of Information Technology</td>
<td></td>
</tr>
</tbody>
</table>
PURPOSE

This control is intended to establish the policy and procedures for security awareness training in order to identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

REQUIREMENTS

NSU provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and annually or more often as necessary thereafter.

1. Develop an information security training program so that each IT system user is aware of and understands the following concepts:
   
   a. The University's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
   
   b. The concept of separation of duties;
   
   c. Prevention and detection of information security incidents, including those caused by malicious code;
   
   d. Proper disposal of data storage media;
   
   e. Proper use of encryption;
   
   f. Access controls, including creating and changing passwords and the need to keep them confidential;
   
   g. Agency acceptable use policies;
   
   h. Agency Remote Access policies;
   
   i. Intellectual property rights, including software licensing and copyright issues;
   
   j. Responsibility for the security of COV data;
   
   k. Phishing; and
   
   l. Social engineering.

2. Require documentation of IT system users’ acceptance of the University’s security policies after receiving information security training.
Supplemental Guidance: The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to NSU’s information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior University officials, displaying logon screen messages, and conducting information security awareness events.

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 62.8.202

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard