Policy Title: Use of External Information Systems

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 120 (2014) Use Of External Information Systems

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

NSU may utilize external information systems at the University’s discretion in accordance with applicable Commonwealth laws and regulations. The following conditions outline the acceptable use policy for these external systems.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Contacts</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<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>4</td>
</tr>
<tr>
<td>Related Documents</td>
<td>4</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869
ADMINISTRATIVE POLICY # 32 – 8 – 120 (2014) Use Of External Information Systems

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology

PURPOSE

This control is intended to address policy and procedures for the use of external information systems in regard to access and information handling.

REQUIREMENTS

NSU establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from the external information systems; and
2. Process, store, and/or transmit University-controlled information using the external information systems.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by NSU and for which NSU typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); NSU establishes terms and conditions for the use of external information systems in accordance with NSU security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the University information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system.

NSU will identify whether personal IT assets are allowed onto premises that house IT systems and data, and if so, identify the controls necessary to protect these IT systems and data.

Control Enhancements for Sensitive Systems:
1. NSU permits authorized individuals to use an external information system to access the information system or to process, store, or transmit University-controlled information only when NSU:

   a. Can verify the implementation of required security controls on the external system as specified in NSU’s information security policy and security plan; or

   b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

2. NSU limits the use of University-controlled portable storage media by authorized individuals on external information systems.

   Enhancement Supplemental Guidance: Limits on the use of University-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

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 62.8.120 Use of External Information Systems

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard