Policy Title: Transmission Confidentiality

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1609 (2014) Transmission Confidentiality

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Transmission integrity addresses the security controls used to ensure the confidentiality of communications across internal and external networks the University employs for its information system.

**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>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 transmission confidentiality on the networks employed by the University’s information system.

REQUIREMENTS

The information system protects the confidentiality of transmitted information.

NSU requires encryption for the transmission of email and attached data that is sensitive relative to confidentiality. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.

Supplemental Guidance: This control applies to communications across internal and external networks. If the University is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the University either implements appropriate compensating security controls or explicitly accepts the additional risk.

Control Enhancements for Sensitive Systems:

1. NSU employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by University-defined alternative physical measures.

   Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

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 – 1609 (2014) Transmission Confidentiality

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 62.8.1609 Transmission Confidentiality

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard