Policy Title: Use of Cryptography

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1613 (2014) Use of Cryptography

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

The use of cryptography, for both internal and external transmissions, plays a critical role in ensuring integrity, confidentiality, and authenticity of communications throughout University’s 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>1</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>4</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

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology
PURPOSE

This control is intended to establish the policy and procedures for the use of cryptography on the University’s information system.

REQUIREMENTS

The information system implements required cryptographic protections using cryptographic modules that comply with applicable laws, directives, policies, regulations, standards, and guidance.

Commensurate with sensitivity and risk, NSU or its service provider shall:

1. Define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data.

2. Document appropriate processes before implementing encryption. These processes must include the following components:
   a. Instructions in the IT Security Agency’s Incident Response Plan on how to respond when encryption keys are compromised;
   b. A secure key management system for the administration and distribution of encryption keys; and
   c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.

3. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-NSU networks or any publicly accessible networks, or any transmission outside of the data’s broadcast domain. Digital signatures may be utilized for data that is sensitive solely relative to integrity.

Examples of Sensitive or Confidential University Information:

Some examples of sensitive data include social security numbers, credit card numbers, medical history, certain financial data, and other data as defined by FERPA, HIPAA, the Commonwealth of Virginia, or other relevant laws and regulations. Directory information is not considered sensitive.

Acceptable Encryption Standards

The use of proprietary encryption algorithms is not allowed for any purpose unless it has been reviewed by qualified experts and approved by the University's duly appointed Information Systems Security Officer.
Proven standard Encryption methods such as AES, Blowfish, RSA, RC5, IDEA, etc., and encryption keys of 128 bits or higher must be used when encrypting sensitive data.

A One-Way Hash Function must be used to irreversibly encrypt digital signatures, integrity checksums, authentication information including passwords, and similar types of data.

User Responsibilities

Users who have access to sensitive and confidential information are authorized and expected to encrypt data for protection against unauthorized disclosure both while it is being stored and while it is being transmitted as well.

Users must protect sensitive and confidential information wherever it resides - on servers, desktop and laptop personal computers, and even when or if it is placed onto peripheral storage devices such as PDA's, USB/thumb drives, memory cards, computer diskettes and discs, media players, digital cameras, cell phones, etc.

Users must ensure they properly secure any encryption keys associated with encrypted data.

Users must be aware that the U.S. Government has restricted the export of encryption technologies. Those users who are residents of other countries and those who travel to foreign countries must also be aware of the encryption technology laws of those countries as well.

Users who have questions or require assistance concerning encryption should send an e-mail to helpdesk@nsu.edu or call the OIT Help Desk on 823-8678.

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 62.8.1613 Use of Cryptography

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard