Policy Title: Identification and Authentication (University Users)

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 702 (2014) Identification and Authentication (University Users)

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Comprehensive and well-defined identification and authentication policies are necessary to maintain a secure information system. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The University risk management strategy is a key factor in the development of an identification and authentication policy.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</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 establishes the University’s policy for maintaining and managing identification and authentication for University users.

REQUIREMENTS

The information system uniquely identifies and authenticates University users (or processes acting on behalf of University users).

Supplemental Guidance: University users include NSU employees or individuals NSU deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the University. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to University information systems is defined as either local or network. Local access is any access to a University information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an University information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the University. For a virtual private network (VPN), the VPN is considered an internal network if the University establishes the VPN connection between University-controlled endpoints in a manner that does not require the University to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted.

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 62.8.702 Identification and Authentication (University Users)

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard