Policy Title: Least Privilege

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 106 (2014) Least Privilege

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Least privilege is a concept that is implemented in order to reduce risk to University operations by only allowing the necessary access for any given user to accomplish the tasks associated with their role or responsibility.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Contacts</th>
<th>1</th>
</tr>
</thead>
<tbody>
<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>3</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>3</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 for the use of least privilege with regard to user’s access permissions on the University’s information system.

REQUIREMENTS

NSU employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with University missions and business functions.

Supplemental Guidance: NSU employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to University operations and assets, individuals, and other organizations.

Control Enhancements for Sensitive Systems:

1. NSU explicitly authorizes access to administrative accounts.

   Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

2. NSU requires that users of information system accounts, or roles, with access to administrative accounts, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

   Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role Based Access Control (RBAC) is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.
3. NSU limits authorization to super user accounts on the information system to designated system administration personnel.

4. NSU prohibits privileged access to the information system by non-University users

   Enhancement Supplemental Guidance: A qualified University user may be advised by a non-University user, if necessary.

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 62.8.106 Least Privilege

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard