Policy Title: Physical Access Control

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1103 (2014) Physical Access Control

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Physical access control involves the University’s capacity to maintain regulation of access to its information system. Administering and monitoring of this access is necessary to reduce risk of threat to the information system and its components.

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>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>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 of physical access control to the University’s information system.

REQUIREMENTS

NSU:

1. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

2. Verifies individual access authorizations before granting access to the facility;

3. Controls entry to the facility containing the information system using physical access devices and/or guards;

4. Controls access to areas officially designated as publicly accessible in accordance with the University’s assessment of risk;

5. Secures keys, combinations, and other physical access devices; and

6. Inventories physical access devices at least annually.

NSU shall safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).

Supplemental Guidance: NSU determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) a University information system may be located in areas designated as publicly accessible with access to such devices being safeguarded.

Control Enhancements for Sensitive Systems:

1. NSU enforces physical access authorizations to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within a University facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the University may be more vulnerable due to the concentration of information system components.
VIOLATIONS

Violations of this policy will be addressed in accordance with 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 62.8.1103 Physical Access Control

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard