Policy Title: Access Control for Mobile

Policy Type: Administrative


Approval Date: 05/20/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Mobile devices, both personal and University-controlled, are subject to NSU network access policies when connected to the University information system. The following conditions further govern the use, accessibility, and monitoring all mobile devices are subject to on University networks.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Contacts</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<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>3</td>
</tr>
<tr>
<td>Interpretation</td>
<td>4</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 requirements regarding access control for mobile devices in order to help mitigate risk from malicious or otherwise compromised devices to the University’s information system.

REQUIREMENTS

NSU:

1. Establishes usage restrictions and implementation guidance for University-controlled mobile devices;

2. Authorizes connection of mobile devices meeting University usage restrictions and implementation guidance to University information systems;

3. Monitors for unauthorized connections of mobile devices to University information systems;

4. Enforces requirements for the connection of mobile devices to University information systems;

5. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

6. Issues specially configured mobile devices to individuals traveling to locations that the University deems to be of significant risk in accordance with University policies and procedures; and

7. Applies University-defined quarantine, inspection and preventative measures to mobile devices returning from locations that the University deems to be of significant risk in accordance with University policies and procedures.

Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). University-controlled mobile devices include those devices for which NSU has the authority to specify and the ability to enforce specific security requirements. Usage
restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay. University policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

Control Enhancements for Sensitive Systems:

1. NSU restricts the use of writable, removable media in University information systems.

2. NSU prohibits the use of personally owned, removable media in University information systems.

3. NSU prohibits the use of removable media in University information systems when the media has no identifiable owner.

   Enhancement Supplemental Guidance: An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

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 62.8.119 Access Control for Mobile Devices

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard