Policy Title: Wireless Access

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

Wireless connectivity, including but not limited to, microwave, satellite, Bluetooth, and WIFI is maintained and monitored by the NSU OIT team. All connections are subject to following conditions.

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>5</td>
</tr>
<tr>
<td>Interpretation</td>
<td>5</td>
</tr>
<tr>
<td>Publication</td>
<td>5</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>5</td>
</tr>
<tr>
<td>Related Documents</td>
<td>5</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 access and restriction in regard to wireless accessibility of both University internal and general use networks.

REQUIREMENTS

NSU:

1. Establishes usage restrictions and implementation guidance for wireless access;
2. Monitors for unauthorized wireless access to the information system;
3. Authorizes wireless access to the information system prior to connection; and
4. Enforces requirements for wireless connections to the information system.

Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization controlled facilities.

NSU’s ISO is accountable for ensuring the following steps are followed and documented:

Wireless LAN (WLAN) Connectivity on the NSU Network:

1. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal University network.
   a. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);
   b. WLAN infrastructure must authenticate each client device prior to permitting access to the WLAN;
   c. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;
   d. Only University owned or leased equipment shall be granted access to an internal WLAN;
e. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);

f. Physical or logical separation between WLAN and wired LAN segments must exist;

g. All University WLAN access and traffic is monitored for malicious activity, and associated event log files stored on a centralized storage device;

h. Configuration and security data associated with the WLAN will not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and

i. WLAN clients will only permit infrastructure mode communication.

WLAN Hotspot (Wireless Internet):

2. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:

   a. WLAN Hotspots must have logical or physical separation from the University’s LAN;

   b. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;

   c. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and

   d. Where University clients are concerned, WLAN clients will only permit infrastructure mode communication.

Wireless Bridging:

3. The following network configuration shall be used when bridging two wired LANs:

   a. All wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption methods (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);

   b. Wireless bridging devices will not have a default gateway configured;
c. Wireless bridging devices must be physically or logically separated from other networks;

d. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;

e. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and

Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point)

Control Enhancements for Sensitive Systems:

1. The information system protects wireless access to the system using authentication and encryption.

   Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary.

2. NSU monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, and takes appropriate action if an unauthorized connection is discovered.

   Enhancement Supplemental Guidance: The University proactively searches for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

3. NSU disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

4. NSU does not allow users to independently configure wireless networking capabilities.

   Enhancement Supplemental Guidance: Wireless capabilities include the access points, authentication controllers, antennae, etc. This control is not intended to restrict the use of client software on desktops or laptops to connect to authorized wireless networks. NSU does not allow users to create ad-hoc, or decentralized, networks.
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 62.8.118 Wireless Access

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard