Wireless Standards Policy

Policy Number:
Owner Department: Information Technology
Effective Date: February 24, 2011
Approved By: President's Council

I. POLICY TITLE

Wireless Standards Policy

II. POLICY STATEMENT

A. The Information Technology department will be solely responsible for the deployment and management of wireless standards access points on campus. No other departments or individuals may deploy wireless networks or wireless access points. This includes all intra-building and inter-building wireless LAN communications.

B. Wireless Local Area Networking using the IEEE 802.1xx standard is a rapidly-evolving, easy to deploy technology, but highly sensitive to interference and overlapping frequencies. In addition, sensitive information can easily be compromised when wireless equipment is configured without industry accepted security protocols. These characteristics require that all wireless use at SCNM be planned, deployed, and managed in a very careful and centralized fashion to ensure consistent and reliable functionality, acceptable levels of performance, and all appropriate security and accountability features.

III. POLICY STATUS

New

IV. DEFINITION(S)

None

V. PURPOSE

To ensure the technical coordination required to provide the best possible wireless network for SCNM, this policy:

a. provides the structure for a campus-wide implementation of wireless technology
b. identifies responsibility for the deployment and management of the wireless network
c. identifies the wireless protocols, security and devices in use on campus
d. identifies security measures and installation procedures

Wireless Standards Policy

VI. SCOPE/KEY STAKEHOLDERS

Stakeholders are defined as SCNM software users: Faculty, staff, and students

VII. POLICY ITEMS

A. Each access point shall support encrypted connections and may or may not also support an unencrypted mode.
B. The encrypted network shall utilize the following standards to guarantee the highest levels of security for standard users:
    a. Security Mode: WPA or successor protocol
    b. Encryption: AES or successor protocol
       IEEE 802.IX with Protected Extensible
       TKIP or successor protocol
    c. Client Limitations: Not compatible with all hardware or operating systems
C. Wireless networks shall be configured in compliance with industry standard best practices for the relevant security models.
D. Security Infrastructure and User Accounts
    a. The primary information source for wireless users shall be at http://my.scnm.edu/ics . This site provides client configuration guides for supported operating systems, instructions for activating wireless accounts, and any other information deemed necessary or appropriate.
E. Wireless Bridging
    a. All building-to-building network connections, wired or wireless, are the responsibility of IT. Secured wireless bridges may be proposed as a connection medium for sites where fiber-optic or DSL connections are impractical. All such scenarios will be reviewed by the IT on a case-by-case basis. Under no circumstances shall any building-to-building network connection be maintained by any entity other than IT.
F. Ad-Hoc Networking
    a. The use of 802.1xx technologies to directly link two computers without the assistance of an access point can occasionally be a convenience but creates potential security hazards. Therefore Ad-Hoc networking is prohibited.
G. Unauthorized Devices
    a. All wireless infrastructure devices except those deployed under IT are forbidden on College property. Any such rogue devices already existing must be removed from service. When IT locates a rogue access point on college grounds, the device will be disconnected and instructions to contact IT will be left for the owner. Any rogue device which is returned to service in defiance of these instructions is subject to physical removal.
H. Wireless Support and Troubleshooting
    a. Faculty and staff shall report wireless networking trouble through the IT Help Desk. Students may receive direct support by visiting the Technology Resource Center. Access point failure or interruptions of wireless service shall be addressed by the IT team as with any other network infrastructure outage.

Wireless Standards Policy

VIII. RESPONSIBILITY FOR IMPLEMENTATION

Network Administrator

IX. APPROVAL BODY

President's Council

X. DATE POLICY APPROVED

February 23, 2011

XI. RELATED POLICIES

IT Acceptable Use Policy

XII. RELATED DOCUMENTS

None

XIII. DATE EFFECTIVE

February 24, 2011

XIV. NEXT REVIEW DATE

As needed

XV. VERSION CONTROL AND CHANGE HISTORY

Version Control	Approved By/Date	Date Effective	Amendment
1	President's Council/ February 23, 2011	February 24, 2011	
2			

XVI. POLICY OWNER

Information Technology Department

XVII. POLICY AUTHOR/CONTACT

Stan Zalewski/Director IT