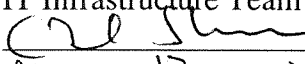


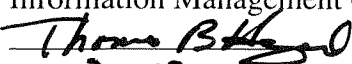
**MEDICAL UNIVERSITY OF SOUTH CAROLINA
OFFICE OF THE PRESIDENT
POLICY MEMORANDUM**

Memorandum ID: OP-2003-001-Information Systems

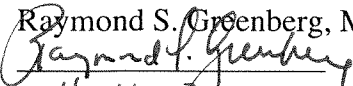
Title: Wireless Networking Policy

Originator: C. Frank Starmer, PhD
Date: March 4, 2003

Reviewed: IT Infrastructure Team
Approval: 
Date: March 17, 2003

Reviewed: Information Management Council
Approval: 
Date: 3-18-03

Implementation: CCIT
Date: Immediately upon approval

Approved: Raymond S. Greenberg, MD, PhD
Approval: 
Date: 4-11-03

Distribution: University-wide

RATIONALE

Wireless networking technologies can allow MUSC staff to access networked information from any portable PC or handheld device, without the restrictions on location imposed by wired connections. Wireless mobility can support diverse applications, ranging from more efficient bedside patient care, to new forms of teaching and learning in the classroom. At the same time, the broadcast nature of wireless (radio) communications raises security concerns, and carries the potential for interference between neighboring devices, if wireless devices are installed and used naively. For these reasons, any wireless Access Point (AP) which is connected to the campus network must be treated as an extension of the campus network.

This policy applies to all use of 802.11 wireless networking devices on the MUSC network. All other policies covering the use of University computing services by authorized users (e.g. the MUSC Computer Use Policy) are still in effect when resources are accessed from wireless devices, as are all regulations (e.g. HIPAA and FERPA) which protect the confidentiality and integrity of information entrusted to the University's stewardship.

POLICY

Wireless APs will be centrally managed like all other parts of MUSC's network infrastructure. No Access Point (implementing 802.11 or any other wireless networking standard) may be connected to the MUSC network except as authorized by the Network Systems Team (NST) in the Center for Computing and Information Technology (CCIT).

GUIDELINES

Network Topology

NST will configure every connected AP onto a dedicated "Wireless VLAN" whose primary purpose is to prevent access to the wired segments of the MUSC network by unauthenticated mobile users.

User Authentication

All users connecting to any AP on the MUSC network must be authenticated using an approved authentication service. Information on currently approved and operational authentication services is available from NST.

Data Encryption

All sensitive information traversing wireless links connected to the MUSC network must be protected using an approved encryption method. Information and guidelines on currently approved encryption methods is available from NST.

Audits

CCIT will maintain access logs for all wireless APs connected to the MUSC network. CCIT will also conduct periodic audits throughout MUSC's airspace to ensure that APs have not been attached to MUSC's network without authorization. Any unauthorized APs will be removed, and the person(s) responsible for them will be subject to sanctions as outlined in the MUSC Computer Use Policy.

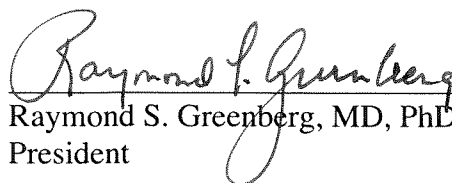
Procurement and Installation

Persons planning to enable wireless access to the MUSC network must contact CCIT's Network Systems Team prior to purchasing or installing any equipment. NST's engineers will facilitate the procurement of APs and other equipment from an approved equipment list, and will install, configure and manage all APs in accordance with applicable networking and security policies and standards. NST's engineers will also help ensure that APs are placed to maximize coverage and minimize interference, and will facilitate the sharing of APs between neighboring departments and programs where feasible.

ACCESS

This policy will be available from the Office of the President. It will be distributed digitally and by hardcopy to the administrative officers of all units reporting to the President, and be maintained on an accessible web site under MUSC's Home page, <www.musc.edu>. The President, or a designee, will be responsible for monitoring and maintaining this policy. This policy will be reviewed for revision as appropriate. This memorandum is a public document and has no restriction on its distribution.

Signed:


Raymond S. Greenberg, MD, PhD
President