UMDNJ
University of Medicine & Dentistry of New Jersey

INFORMATION SERVICES & TECHNOLOGIES
ENABLING THE ENTERPRISE

Wireless LAN Policy

Approved:	September 6, 2008	**Amended:**	
Effective:	September 10, 2008	**Expires:**	
Version:	95-01-01-08		

I. PURPOSE

To establish policy defining the requirements associated with access to, and usage of, the UMDNJ Wireless network.

II. Accountability

The Vice President of Information Services and Technology (IST), IST Director(s) and school / unit IT Management shall ensure compliance with this policy.

III. APPLICABILITY

This policy applies to any wireless device used to establish any connectivity to UMDNJ's network. This policy applies to all UMDNJ faculty, staff, students, contractors, vendors and consultants including personnel affiliated with third parties. It is also applicable to all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) that have the ability to connect to any of UMDNJ's networks. This includes any form of wireless communication device capable of transmitting packet data.

Policy

There are many technologies available to counteract wireless network intrusion, but currently no method is absolutely secure. IST currently utilizes a number of security measures identified below. Because of the dynamic nature of wireless communications and protocols, IST will periodically address changes and will update documentation accordingly and as needed.

1. Only individual user accounts shall be provided immediate wireless access upon registration. Generic accounts requiring wireless access must be approved by IS&T and follow the generic account policy, prior to wireless access being granted. .

2. All wireless access points connected to the network must be approved and sanctioned by IST in accordance with the IST Wireless Policy and shall employ network security measures defined herein.

3. Rogue access points are proactively identified by IST and are promptly removed from the network in a timely manner

4. All wireless networks are continuously monitored for weaknesses and breaches. IST reserves the right to isolate, quarantine and / or disconnect any non- IST sanctioned wireless device.

IV. Requirements

Physical Security:

A. Wireless Access Point hardware must be approved and configured by IS&T.
B. Hardware shall be located out of reach from potential tampering. (Excluding antennae)

Configuration Security:

A. IEEE 802.1x Port security must be enabled on the wired connection to an access point
B. UMD-WIFI-R SSID broadcasting must be disabled
C. WPA 128-bit encryption is the minimum acceptable encryption standard
D. IEEE 802.1X user authentication against the Active Directory database
E. Network segregation is not applicable. Access to UMDNJ systems is defined on an application basis.

Hardware: All hardware must be capable of, and adhere to the following:

A. Terminate on wireless access points sanctioned by IS&T using approved hardware and configured software, that is procured in accordance with University Purchasing policy, protocol and procedure. The current IST standard is Cisco Aironet 1200 series access points.

B. Maintain point-to-point hardware encryption of at least 128 bits for transmission of all data. Highly confidential data must communicate via 256 bit encryption or above (See the data sensitivity policy). Currently UMDNJ utilizes the LEAP and PEAP wireless protocols.

C. Maintain a unique identifier that can be registered and tracked, i.e., a Media Access Control (MAC) address assigned to the computer's network identification card (NIC).

D. Support strong user authentication such as certificates, one time passwords, or authentication against an external database such as TACACS+, RADIUS or something similar.

E. Obtain approved access through the central registration system. All related policies must be read, understood and accepted with signature (this may require discussion as the process will change) before access is provided. Only individuals with a Reserved User ID (RUID) will be granted immediate access. Generic and temporary accounts will require IS&T approval before being permitted to connect to the UMDNJ wireless network.

F. All devices and users must authenticate against the IS&T central Active Directory database. Usernames and passwords must conform to the requirements set forth by IS&T policy and procedure.

G. Maintain secure access to UMDNJ networks. Only those devices explicitly approved and configured by IS&T can be used to establish over the air connectivity. Rogue (non- IST sanctioned) wireless devices jeopardize the overall security of the network, are not permitted, and will be removed from the network.

H. Comply with all other applicable UMDNJ and IST policies.

Glossary of Terms:

Cisco Aironet 1200: is a single band lightweight or autonomous access point

Encryption / De-Encryption - A secure method to send a message in encrypted code. The only method able to decode the message is a receiver with the correct encrypt/de-encrypt key. This adds a layer of security to

the data conversation because if it is intercepted the message looks like a random series of letters, numbers, and characters.

IEEE 802.1x –: a generic solution for port security that can be applied to virtually any wired or wireless network for port authentication.

LEAP uses TKIP and dynamic WEP keys rather than PKI and TLS for authentication confidentiality.

Network segregation: separates one Network into two LANs

PEAP uses server-side PKI to build an encrypted EAP-TLS tunnel between the client and server prior to the client transmitting its authentication credentials (username, password, certs, etc.).

Rogue device- Any device not authorized for use on the UMDNJ network RUID (Reserved University Identification) – Unique UMDNJ reserved ID to identify an individual or object.

TACACS+ and RADIUS: security protocols used to control access into networks

UMD-WIFI-R SSID broadcasting: This feature will broadcast the network name, making it easier to detect for unauthorized entry. With the feature disabled, the detection of the network becomes more difficult for the unauthorized user to obtain access

User authentication – A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

WPA 128-bit encryption: Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). A major improvement in the protocol over WEP (Wired Equivalency Privacy) key.

VI. NON-COMPLIANCE AND SANCTIONS

Any person(s) found to have violated this policy may be subject to removal of access privileges to the University network; disciplinary action under applicable University policies and procedures up to and including termination; civil litigation; and/or criminal prosecution under applicable state and federal statutes.