



SECTION: INFORMATION TECHNOLOGY

AREA: GENERAL

SUBJECT: WIRELESS NETWORKING

I. INTRODUCTION

This Policy governs wireless networks within the University of Arkansas for Medical Sciences (UAMS). Wireless networks allow users to access computing facilities and information resources from portable and mobile devices. They also facilitate extending network connectivity to locations that are not feasible to hard wire (temporary facilities, cost prohibitive locations, etc.)

II. GENERAL PROVISIONS

A. PURPOSE

The purpose of this Policy is to:

- Ensure that UAMS wireless resources are used for purposes appropriate to the UAMS mission and goals;
- Prevent disruptions to and misuse of UAMS wireless resources;
- Assign responsibility for the administration of the wireless radio frequency spectrum defined in the **IEE 802.11** standards and the deployment of wireless resources;
- Ensure that the UAMS community is aware that use of UAMS wireless resources is subject to state and federal laws and UAMS policies; and
- Ensure that wireless resources are used in compliance with those laws and UAMS policies.

B. SCOPE

This Policy applies to:

- All wireless network resources owned or managed by UAMS;
- All wireless network resources provided by UAMS through contracts and other agreements with UAMS;
- All wireless network resources located within UAMS owned or leased facilities;
- All users and uses of any wireless and wired network resources at UAMS.

C. DEFINITIONS

Access Points (APs): Electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a Local Area Network (LAN), using antennas to transmit and receive instead of ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the UAMS network backbone.

Compelling Circumstances: Circumstances in which time is of the essence or failure to act might result in personal injury, property loss or damage, adverse effects on UAMS resources or services, loss of evidence of one or more violations of law or of UAMS policies or liability to UAMS or to members of the UAMS community.

Coverage: The geographical area where a baseline level of wireless connection service quality is attainable.

Encryption: The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption).

Interference: The degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.

Password: A string of characters which serves as authentication of an individual's identity, which may be used to grant, or deny, access to private or shared data.

Rogue Access Point: Any wireless device that is operating in the 2.4Ghz or 5Ghz radios frequency range that is not managed by the UAMS IT Network Engineering department.

Wireless Hardware/Software: The electronic equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device to provide an interface to a wireless network.

IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the **Institute of Electrical and Electronics Engineers (IEEE)** Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.

Wireless Network: A local area network technology that uses radio frequency spectrum and adheres to the IEEE 802.11 Standard while connecting computing devices to UAMS wired networks and the Internet.

Wireless Resources: Wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless network and the devices that connect wirelessly to it.

D. VIOLATIONS OF LAW AND POLICY

UAMS considers any violation of this Policy and/or law to be a serious offense and reserves the right to copy and examine any files or information resident on UAMS wireless resources to ensure compliance. Violations of this policy should be reported to the appropriate UAMS authority.

Sanctions of Law. Both federal and state laws prohibit theft or abuse of wireless resources. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of wireless resources. Any form of harassing, defamatory, offensive, illegal, discriminatory, obscene, or pornographic communication, at any time, to any person is also prohibited by law. Violations of the law may result in criminal penalties.

Disciplinary Actions. Violators of this Policy and/or law may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable UAMS policies.

E. NO EXPECTATION OF PRIVACY

There is no expectation of privacy in the use of wireless resources at UAMS. UAMS reserves the right to inspect, monitor, and disclose all wireless resources including files, data, programs and electronic communications records without the consent of the holder of such records.

III. SUITABILITY

Wireless networking is not a strategic replacement for a wired network. The capabilities and security provided through wired network technologies will likely continue to outpace improvements in capabilities provided by wireless network technology. A wireless network must be an augmentation of a wired network.

The FCC does not license use of the frequencies used by wireless devices and therefore other devices that use the same frequencies may disrupt wireless communications. These devices include but are not limited to cordless phones, microwave ovens and personal network devices. Areas with high interference from such devices may not be suitable for wireless networks.

Many devices and equipment that are available for purchase have wireless features built in that could interfere with the UAMS wireless network. Any purchase request for devices or equipment that have wireless capability must be reviewed and approved by the

UAMS IT Technical Support Center to ensure they will not interfere with the wireless network.

IV. ADMINISTRATION

Wireless Networks will:

- Be centrally administered as a component of the LAN.
- Be regularly scanned for rogue APs and have those removed immediately.
- Adhere to health, building, and fire codes.
- Comply with all federal and state regulations for wireless communications.
- Use supported radio frequency bands.

Access Points must:

- Be adequately secured from theft, vandalism, and unauthorized data port access.
- Have upgradeable firmware.
- Have wireless access to the administration port disabled at all times.
- Where necessary, have passwords changed initially and at regular intervals thereafter.
- Require authentication before granting access.
- Be configured with encryption enabled; where encryption keys must be changed at regular intervals and must not be posted publicly.
- Be purchased, owned, and operated by the UAMS Information Technology (IT) department.

V. ACCESS RESTRICTIONS

Use of the UAMS wireless network may be wholly or partially restricted or rescinded by UAMS without prior notice and without the consent of the user under conditions such as:

- when required by and consistent with law;
- when there is reason to believe that violations of law or UAMS policies have taken or may take place; or
- when there are compelling circumstances.


VI. DISCLAIMER

UAMS disclaims any responsibility for and does not warranty information and materials residing on non-UAMS systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of UAMS, its faculty, staff or students.

VII. NOTICE TO USERS

As laws, technology and standards change from time to time, this Policy may, after appropriate review, be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of UAMS Policies.

SIGNATURE:

A handwritten signature in black ink, appearing to read "Donald Wilson", written over a horizontal line.

Chancellor

Date: December 19, 2008