Policy Statement

Information Technology Services (iTech) for the University of Southern Mississippi is responsible for providing a reliable and secure network service to all campus constituents. This wireless policy has been established to govern all implementations of wireless networks and the general use of wireless technology at Southern Miss and to alert members of the campus community to the potential problems that could result from devices using the same radio frequencies.

Reason for Policy/Purpose

The purpose of the Wireless Policy is to set guidelines for the use of wireless technology by the University of Southern Mississippi’s campus community so that optimum network capabilities for all wireless and wired facilities can be secured and maintained.

This policy should also alert members of the campus community to the potential problems that could result from wireless devices using the same radio frequency.

Who Needs to Know This Policy

All users accessing wireless technology at The University of Southern Mississippi.

Website Address for this Policy

www.usm.edu/institutional-policies/policy-acaf-it-023

Definitions

network An interconnected group of computers. Networks may be
classified by the network layer at which they operate according to basic reference models considered as standards in the industry. The majority of networks use the Internet Protocol Suite (IP). Southern Miss utilizes a LAN and WAN network.

LAN network
A LAN network covers a small geographic area, such as the Southern Miss campus.

WAN network
A WAN is a data communications network that covers a relatively broad geographic area (i.e. one city to another and one country to another country) and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

wireless devices
Any device that utilizes wireless technology such as but not limited to cordless phones, blue tooth devices, wireless gaming controllers, microwave ovens, etc.

Policy/Procedures

1.0 Responsibility
iTech is charged with the responsibility for managing the infrastructure of the Southern Miss Network, this includes the installation, operation, and security of the University’s wireless network.

2.0 Governing Guidelines
2.1 iTech Security and Network Administration and all appropriate local network administrators must approve all wireless network access points prior to installation. Wireless access points may not be installed without prior approval. Unapproved wireless access points are subject to removal.
2.2 Production wireless network access will be provided by iTech in conjunction with appropriate local network support staff. Production wireless access includes all access other than those access points specifically installed to support University sanctioned research into wireless technologies.
2.3 Production wireless network access will require authentication. iTech will design, implement, and manage security authentication schemes.
2.4 Individuals and groups that are pursuing sanctioned research into wireless technologies will be provided specific radio frequency spectra for their wireless access points by iTech. These access points can be attached to the Southern Miss network only in coordination with the iTech.
2.5 iTech will work to accommodate research needs and attempt to eliminate situations of interference between research and production implementations. However, iTech has full
authority to deactivate or require modification in the research wireless network to prevent such interference.

2.6 Any effort to circumvent the security systems designed to prevent unauthorized access to any Southern Miss wireless network may result in the suspension of all access to Southern Miss networks and an appearance before the appropriate disciplinary board.

2.7 The Information Technology Services (iTech) is charged with providing a stable and secure campus network to support the mission of the University and therefore has the authority and responsibility to specify technical requirements for devices connecting to it. This includes providing leadership in the management of shared network resources, such as setting security standards and disconnecting noncompliant wireless devices when they have the potential for interfering with the proper operation of the campus-wide network.

2.8 If our current wireless network doesn’t meet specific departmental needs, iTech can be contacted by submitting a work order to assess the needs.

3.0 Enforcement

3.1 Faculty, Staff, and Students
Any student, faculty, or staff member found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion and/or termination of employment in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.

3.2 External Entities
Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

Review

The Chief Information Officer is responsible for the review of this policy every four years (or whenever circumstances require immediate review).

Forms/Instructions

N/A

Appendices

N/A

Related Information

N/A
History

1. 06/16/08: Policy created.

Amendments: Month, Day, Year – summary of changes
Authorization

WIRELESS NETWORKING POLICY
ACAF-IT-023

As the Responsible Officer, I have reviewed this policy and believe it represents the current policy.

[Signature]

Responsible Officer

4/30/13

Date