Policy for Secure Deployment and Management of IEEE 802.11 Wireless Local Area Networks and other Wireless Standards

Rationale and Purpose of Policy.

To ensure the technical coordination required to provide the best possible wireless network access for the University of Missouri – Kansas City (UMKC), UMKC Information Services (UMKC IS) will be solely responsible for the deployment and management of IEEE 802.11 (802.11) Wireless Local Area Networks and other wireless standards access points on the campus. No other departments may deploy 802.11 or other wireless standards access points.

This policy provides the structure for a campus-wide solution for the implementation of wireless technology, which includes centralized determination of identity and authentication to insure the appropriate levels of security for UMKCnet and the university community.

Wireless in the Local Area Network using the IEEE 802.11 standard is a fast emerging technology based on existing radio frequency technologies. 802.11 wireless technologies are by nature easy to deploy, but highly sensitive to overlapping frequencies. Because of these characteristics, all wireless use must be planned, deployed, and managed in a very careful and centralized fashion to ensure basic functionality, maximum bandwidth, and a secure network. It is not feasible to allow individuals to install their own access points without centralized management, due to the resulting signal interference and greatly degraded performance to the common wireless network and UMKCnet as a whole.

Wireless access points must be tied to authentication security services provided by UMKC IS. Access points which have not been installed by UMKC IS are a security risk by permitting unauthenticated public use of the access point.

Wireless networking technology shares frequency assignments with other consumer products (subject to FCC regulations). Frequency interference may be an issue on campus. UMKC IS will work with all parties involved to arbitrate the issue and seek the best solution in the University’s interest.
Wireless Network Security Policy

Scope.

The Wireless Policy provides guidelines regarding the following:

- The central deployment by IS of 802.11 and related wireless standards access points.
- The provision of wireless service by UMKC IS for campus departments.
- The management by IS of 802.11 and related wireless standards access.
- The management by IS of shared (unlicensed) frequency spectrum on campus.

Policy.

1. UMKC IS deployment of 802.11 and related wireless standards access points
UMKC IS will be solely responsible for the deployment and management of 802.11 and related wireless standards access points on the campus. No other departments may deploy 802.11 or related wireless standards wireless access points. However, departments presently using wireless access points that have not been installed by UMKC IS at the time of the implementation of this policy, UMKC IS will replace the access point with a standardized unit that will be managed by UMKC IS at no cost to the department. A department or unit may turn an unauthorized access point into UMKC IS, and UMKC IS will replace the unauthorized device with an authorized device if the operation of the device is necessary to accomplish department or unit goals. This turn-in period expires on June 1st, 2006. Any unauthorized device (unauthorized wireless device) will be disabled and removed from the network, and may be turned in for replacement during the replacement period.

2. Provision of wireless service by IS
IS will offer a standard wireless deployment plan that will meet the needs of most UMKC departments wishing to construct and operate departmental wireless services. Departments requiring a different wireless deployment plan may contract with IS, if the spectrum is available for it, for premium wireless services. IS will work with departments to accommodate any special needs they may have within the technical constraints of the wireless technology, understanding that all requests may not be technically feasible.

3. Management by IS of 802.11 and related wireless standards access points
IS will ensure that all wireless services deployed on campus will adhere to campus-wide standards for access control. IS will manage the wireless spectrum in a manner that ensures the greatest interoperability and roaming ability for all departments wishing to use wireless technology, and, using the Active Directory, will centralize the process of determining identity, authentication, and appropriate levels of security for access to and use of wireless technology. UMKC IS reserves the right to minimize interference to the common wireless network.

4. Future wireless technologies
This policy will apply to future wireless technologies that allow any type of sharing of network services.
This policy will be updated as needed to address new technologies, as they become available, that impact UMKCnet.

Procedures and Guidelines.

UMKC IS will inform the Provost or designate on wireless plans, deployment strategies, and management issues.

All units must work with UMKC IS to deploy wireless access, and can contact the Call Center at 816-235-2000 to start this process.

In the case of existing wireless technology deployments that use the same or interfering spectrums, UMKC IS will work with the departments in question to minimize interference to the common wireless network.

All sensitive data being transmitted across a wireless network must be encrypted in transit using additional encryption technologies beyond WEP, such as IPsec, SSL, or encrypted VPN technologies.

Sensitive data that must be encrypted in transit would include, but is not limited to:
- Credit Card transactions
- Social Security Numbers
- Student FERPA protected information
- HIPPA protected data

Responsible Organization.

The ITC will be responsible for this policy and for any appeals of UMKC IS decisions relating to wireless deployments. This policy will be reviewed as needed by the ITC. Changes will be authorized by the approval of the Provost or designate. UMKC IS will review LAN wireless access standards on a regular basis and recommend changes to this policy as needed.