Wireless Access Procedure

Introduction
With the proliferation of wireless enabled devices it is necessary to standardize the delivery of wireless network access to promote and maintain the security of the Texas A&M University-Kingsville (TAMUK) network.

Purpose
The purpose of this procedure is to establish rules for governing wireless networking at TAMUK. This procedure limits interference with the University's network infrastructure, promotes greater security in campus networking, and supports the academic mission of the University in order to provide reliable and secure wireless network access.

Audience
This procedure applies to wireless network users at TAMUK.

Wireless Access Procedure
1. Management of Radio Frequencies
   a. TAMUK reserves the right to govern unlicensed radio frequencies within its boundaries. iTech is responsible for managing these radio frequencies and may restrict the use of any devices that can cause interference in the unlicensed radio frequency ranges. These include cordless phones, microwave ovens, and high voltage audio speakers.
   b. iTech is solely responsible for providing wireless networking services on campus. No other department may deploy wireless network access points or other wireless service on campus. Personal or departmental wireless access points are strictly prohibited.
      1) iTech may provide temporary wireless access points to support campus events when possible.
   c. The University will deploy a campus wireless network, based on the 802.11 standards. iTech will work with departments to accommodate specific educational or research applications where technically feasible.

2. Wireless Service Considerations
Wireless services may not be available in all areas of the campus. The wireless network should be viewed as augmenting the wired network, to provide more flexible network use and not as a primary means of network access. Applications that require large amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for wireless access.

3. Security Standards
   a. IEEE 802.1X is the authentication standard. Additional security procedures may be applied as needed.
   b. Wireless users will be required to authenticate with their university provided credentials.
4. Guest Access to the TAMUK Wireless Network  
a. TAMUK offers TAMUK faculty and staff the option of providing guest network logon IDs for their sponsored guests. Guest logon IDs will provide access to TAMUK’s wired and wireless network.  
b. Guests must adhere to all university policies governing the use of information resources. Sponsors provide guest network access on good faith that they will not engage in any illegal or abusive activities while using the TAMUK network, and are ultimately responsible for the actions of their guests.

**Disciplinary Actions**

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

**References**

1. Copyright Act of 1976  
2. Computer Fraud and Abuse Act of 1986  
4. DIR Practices for Protecting Information Resources Assets  
5. DIR Standards Review and Recommendations Publications  
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)  
8. IRM Act, 2054.075(b)  
9. The State of Texas Information Act  
10. The State of Texas Penal Code, Chapters 33 and 33A  
11. Texas Administrative Code, Chapter 202  
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010  
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010  
14. Texas Government Code, Section 441