1. **Purpose**

The purpose of this policy is to establish rules for governing wireless networking at Texas A&M University-Kingsville. This policy 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. This policy applies to all wireless network users at Texas A&M University-Kingsville.

2. **Management of Radio Frequencies**

2.1. Texas A&M University-Kingsville 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.

2.2. 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.

2.2.1. iTech may provide temporary wireless access points to support campus events when possible.

2.3. 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.

3. **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.

4. **Security Standards**

3.1 IEEE 802.1X is the authentication standard. Additional security procedures may be applied as needed.

3.2 Wireless users will be required to authenticate with their university provided credentials.

5. **Guest Access to the TAMUK Wireless Network**

5.1. 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.

5.2. 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.

6. **Disciplinary Actions**

Violation of this policy may result in disciplinary action which may include termination of
employment, dismissal, suspension, or expulsion from an institution of higher education if violated by a student and debarment if violated by a contractor. Additionally, employees, contractors and agents who violate this policy may be subject to loss of TAMUK Information Resources access privileges, and to civil and criminal prosecution.