Wireless networking may pose security risks and management problems. The purpose of the wireless network is to provide a network connection that can be used within limited areas (e.g., a lecture room or meeting room); it is not intended to be a replacement for the wired infrastructure. The following procedures are necessary to preserve the integrity, availability, and confidentiality of electronic information when utilizing wireless connectivity provided by the Texas A&M University Health Science Center (HSC).

1. Wireless Policy

   1.1 Requests for wireless service must be engineered, provided, and maintained by the Office of Information Technology (OIT).

   1.2 OIT will install and maintain all wireless access points, to ensure they meet minimum security requirements.

   1.3 Requests for wireless service for stand-alone or adhoc networks, including but not limited to mobile hotspots, must also be approved by OIT. Devices which negatively impact the HSC wireless infrastructure will not be allowed.

   1.4 Wireless access must be password protected.

   1.5 OIT will monitor for unauthorized wireless access points. Any such rogue access point detected on the HSC network shall be disconnected from the network and a security incident will be filed with the Information Security Officer (ISO), as needed.

   1.6 Confidential information, mission critical or sensitive personal information shall not be accessed by wireless communication unless the communication is encrypted by strong encryption, as determined by the ISO.

   1.7 Information resource security controls must not be bypassed or disabled.

   1.8 The manufacturer default settings of the Service Set Identifier (SSID) shall be changed upon initial configuration of any wireless access device.
All external groups wanting to operate a wireless network in an HSC building or on an HSC campus are required to work with OIT on the deployment of the service.

2. Violations

Violations of this policy may result in disciplinary action, which may include termination for employees and temporary workers; 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 HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration