UTHealth
The University of Texas Health Science Center at Tyler

Origination Date:	*08/2007*
Last Approved:	*10/2016*
Last Revised:	*10/2016*
Next Review:	*10/2019*
Owner:	*John Yoder: VP Information Technology/CIO*
Policy Area:	*Information Resources*
References:	

Wireless Access

Scope

All employees, students, contractors, visitors and consultants at The University of Texas Health Science Center at Tyler (the "University") who access University information resources and networks or access other networks via the University network infrastructure, all data communication systems owned by and/or administered by the University Information Technology (IT)network team, and mobile or stationary computing devices communicating via the University wireless WiFi network. This policy applies to the 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac and future 802.11 wireless standards.

Purpose

To address the security vulnerabilities and responsibilities associated with wireless networking at the University and to establish appropriate procedures to ensure the protection of the existing data communications infrastructure.

POLICY

The University wireless network infrastructure is divided into two distinct networks.

1. **Secure Wireless Network:** This network provides secure authenticated and encrypted access to University internal information such as patient data, e-mail and other applications located within the confines of the University's internal network.
2. **Guest Wireless Network:** This network provides unsecure access to the internet only. Any communications over this network that requires privacy must be done via a virtual private network (VPN) or the secure sockets layer (SSL) protocol. Access to the internal network is prohibited by design and by policy.

The IT network team shall administer the wireless network infrastructure within the University and will install access points (APs) for connecting wirelessly to the data communications network at various locations throughout the University.

All APs shall be of a make, model and design identified and approved by the IT network team. APs will be deployed by the IT network team or approved contractor.

Users are strictly prohibited from installing their own APs within the network. If such devices, considered as 'rogue' APs, are discovered the IT network team reserves the right to render such devices dysfunctional by

blocking access to them. Persistent relocation of rogue APs will result in disciplinary action.

Wireless Network Interface Cards (NICs) installed shall be on the approved list maintained by the IT network team.

While cards from other manufacturers may work, IT is not responsible for providing technical support for cards not on the approved list.

All data communication and activity within the wireless network will be considered untrusted and unsecured unless it has met the security requirements established by the University for secure encrypted wireless communications. Users shall therefore be subject to restrictions implemented to protect the security and integrity of the data communications network if they need to access patient confidential or University private information, including e-mail.

Access to the Internet shall be provided with minimal restriction. However, users accessing Internet services shall be subject to the terms and conditions of the University's Acceptable Use policy.

The active scanning of 802.11b/g, 802.11n, 802.11ac or a future form of wireless data streams for the purpose of finding weaknesses in the integrity of the system with the intent of exploiting such weakness is strictly prohibited. Promiscuous data capture for whatever reason is also strictly prohibited, unless it's required for troubleshooting purposes by the IT network team.

Users shall never assume any privacy when using the Guest wireless service. It is the responsibility of the user to ensure his/her privacy and the protection of privileged information and/or intellectual property.

Attempts to bypass security or to damage the wireless service passively and/or actively are strictly prohibited. Any attempt to physically alter or remove APs by any user other than the IT network team or without the express consent of IT will result in disciplinary action.

Enforcement:

Violation of this policy may result in disciplinary action that may include 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 University Information Resources access privileges, civil, and criminal prosecution.

Attachments:

Approval Signatures

Step Description	Approver	Date
	Kirk Calhoun: President/Prof of Medicine	10/2016
Executive Cabinet	Carol Davis: Executive Assistant, Senior	10/2016
Faculty Senate	Julie Philley: Assoc Prof Of Medicine	10/2016
Office of Legal Affairs	Terry Witter: VP, Legal Affairs/ChiefLegalOf	07/2016
	John Yoder: VP, Information Technology/CIO	07/2016