Wireless Access

Introduction
Information Services (IS) is responsible for providing UTMB with a secure and reliable network infrastructure. With the anticipated proliferation of wireless technology and the potential likelihood of vulnerability and interoperability issues, it is essential that wireless services be coordinated to ensure an acceptable level of security and service for the institution.

Purpose
This practice standard outlines how wireless technologies are to be planned, deployed, managed, and monitored. In addition, this practice standard prohibits attachment or access to the UTMB network via unauthorized or non-compliant wireless communications mechanisms.

Audience
The UTMB Wireless Access Practice Standards apply to all individuals with access to any UTMB Information Resource (IR) and includes all wireless communications devices connected to the UTMB network.

Implications
- To ensure overall network integrity and security, only wireless equipment and services that meet this criteria and supporting IR Security Management Practice Standards are approved for connectivity to the UTMB network.
- To ensure network reliability, IS Network and Security Services (NSS) will manage shared use of the wireless network consistent with shared use of the wired network.
- As with any other UTMB IR, wireless services and equipment are subject to periodic audits and security reviews.
- Pursuant to pertinent policy and practice standards, IS will, at its discretion, disable any unauthorized or non-compliant wireless equipment and services that it discovers on the UTMB network.
Wireless Access, continued

Sensitive Digital Data Management

Sensitive Digital Data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law. Sensitive digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet).

Practice Standards

- Wireless services and equipment will be standardized and must conform to the 802.1x security model for authentication, encryption, and key management.
- IS NSS will identify non-compliant wireless services and disable the equipment. (IS NSS will initially attempt to accomplish this via informing and involving appropriate administration within the business function; however, depending upon the circumstances and the perceived risk, the Information Resources Manager may determine that this action needs to be taken without that cognizance.)
- Wireless services and standards will be centrally managed by IS; all related inquiries and issues should be directed to the IS Help Desk at extension 25200.
- To prevent unauthorized access and easy viewing of data on the internal network, each wireless deployment must enable Wi-Fi Protected Access II (WPA2) or more secure protocol which dynamically generates a new key for each packet transmitted.
- All communications on the internal UTMB wireless network will be encrypted at a minimum of 128 bits; however, users should assume that wireless services in remote locations such as hotels, conference centers, airports, cafes, and at home are not necessarily encrypted and as such remote access requires the use of a Virtual Private Network (VPN).
Wireless Access, continued

Practice Standards (con’t)

- The SSID (service set identifier) for the access point (AP) hardware will be established, registered, configured, and maintained by IS NSS so that it precludes default values. Broadcasting of the internal SSID by the AP must also be disabled. Furthermore, IS NSS will disable the AP from responding to probe-response requests.
- Wireless APs must maintain a hardware address and physical location that is registered with, approved and maintained by IS NSS.
- Users must not set up AP hardware in ad-hoc or stand-alone mode and communicate with each other without traversing an IS authorized AP.
- Users must not extend their own privileges or use of the wireless device for any purpose (e.g., users must not set up workstations and laptops with wireless hardware to act as an AP and advertise wireless services).
- Procedures for guest wireless access (i.e., a secondary wireless network providing temporary Internet access only) will be managed by IS NSS.
- The NSS team will routinely scan the network to identify unauthorized devices. (As with any other IR connected to the UTMB network, this equipment is subject to removal from the network.)
- Perimeter scans will be conducted periodically by the NSS team to determine the extent of radio frequency (RF) broadcast and contain emission within physical boundaries.
- Physical security of wireless equipment must be maintained to provide adequate protection from theft or compromise (preferably APs are installed out of sight).
- Wireless equipment and services are subject to the same policies and practice standards that govern all IR at UTMB including, but not limited to, anti-virus software, platform hardening, authentication mechanisms, timeouts, and encryption.
- Security requirements must be addressed in all phases of the acquisition process and system management lifecycle.
Wireless Access, continued

<table>
<thead>
<tr>
<th>Practice Standards (con’t)</th>
<th>Disciplinary Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Because of the security implications associated with Personal Area Networks (PAN), i.e., Infrared Data Association, (IrDA), Bluetooth, Ultra-wideband (UWB), etc. They will not be used without the approval of the Information Resource Manager.</td>
<td></td>
</tr>
<tr>
<td>● All wireless devices capable of storing digital data, i.e. laptops, desktops, PDA’s, Smart Phones etc. shall use an approved disk encryption controls when storing sensitive data.</td>
<td></td>
</tr>
<tr>
<td>Violations of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil and/or criminal prosecution.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Texas Administrative Code 202.75(W), Wireless Access</td>
</tr>
<tr>
<td>● UTS-165, Information Resource Use and Security Policy</td>
</tr>
<tr>
<td>● NIST 800-48, Wireless Network Security</td>
</tr>
</tbody>
</table>