

Wireless Addendum	 THE UNIVERSITY of TENNESSEE Health Science Center			NETWORK SECURITY		
	Doc. Version:	1.0.0	Page 1 of 2			
	Revised by:	John Baxter	Date:	8/29/04		
	Effective Date:	10/12/2004				
Approval:		W. R. Rice, Chancellor & C. Fitch, CIO				

Overview

Wireless networking is based on the use of unlicensed and widely available radio frequency bands to establish a shared network entity (cell) that can be connected by anyone within range of the cell's access point. Deployment of wireless cells requires that installations carefully avoid interference between devices in different cells. Since common wireless security mechanisms have been shown to be subject to compromise, all wireless traffic should be presumed to be insecure and subject to unauthorized viewing. As a result of these problems, the access of the University network by wireless means requires careful design and installation of wireless infrastructure, authorization of all clients seeking wireless access, and strong authentication of users attempting wireless access.

Purpose

This policy prohibits access to the University networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by UTHSC Network Services are approved for connectivity to the University's networks.

Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the University's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the University's networks do not fall under the purview of this policy.

Definitions

Strong Authentication A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used. Strong authentication requires strong passwords. **(Reference Password Addendum)**

Policy

1. It is a violation of policy to access or attempt to access the University network with unsecured wireless communication.
2. All existing security policies (Acceptable Use, Remote Access, Password, etc.) apply to network access by wireless devices as they do to wired devices.
3. Wireless connections must use end-to-end encryption of at least 128 bits and support strong user authentication that utilizes an external database such as TACACS+, RADIUS, etc.
4. Only approved hardware, software and wireless protocols may be used to access the University's network.

	NETWORK SECURITY		
Wireless Addendum	Doc. Version:	1.0.0	Page 2 of 2
	Revised by:	John Baxter	Date: 8/29/04
	Effective Date:	10/12/2004	
	Approval:	W. R. Rice, Chancellor & C. Fitch, CIO	

5. Wireless clients must maintain a hardware address (MAC address) that can be registered and tracked.
6. Wireless accounts must not be shared.
7. All wireless access points connected to the University network must be engineered, installed, and maintained by UTHSC Network Services or by their designated alternate.

Guidelines

Care should be taken when placing wireless devices in areas containing other equipment such as laboratory instrumentation or patient monitoring equipment. The possibility of radio frequency interference should be tested.

The policy covers all wireless access to include 802.11x and CPDP (Cellular).

Enforcement

Reference **Enforcement** in **Acceptable Use** document

Additional Information

Any inquiries relating to this Wireless Addendum should be directed to the Security Director.