THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: SC-004-Wireless Network Security	
Version 1	**Effective Date: 04/06/2021**

Responsible Office: Office of Cybersecurity	Last Review: 04/07/2021 Next Review: 04/07/2023
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The purpose of this standard is to establish controls for 802.11x wireless networks to minimize risks to the confidentiality, integrity, and availability of information and to support secure access to resources and services over wireless networks.

802.11x wireless networks enable users of wireless devices the flexibility to physically move throughout a wireless environment while maintaining connectivity to the network. While 802.11x wireless networks are exposed to many of the same risks as wired networks, they are also exposed to additional risks unique to wireless technologies. This standard outlines the additional controls required for the use of wireless networks.

Scope

This standard applies to all 802.11x wireless networks that store, process, or transmit data or connect to a UTHSC network or system, including networks managed and hosted by third parties on behalf of UTHSC.

The types of 802.11x wireless networks in scope include:

1. Internal – these wireless networks are directly connected to the internal information technology resources and are only available to authenticated users.
2. Public (authenticated) – these wireless networks are not connected to internal information technology resources and access is limited to authenticated users.
3. Public (non-authenticated) – these wireless networks are not connected to internal information technology resources and are available for anyone to use without authentication.

Definitions

AP – Wireless Access Point – a networking hardware device that allows other wireless devices to connect to a network.

Wi-Fi Protected Access (WPA) – a security protocol designed to create secure wireless networks.

Responsibilities

ITS Networking personnel are responsible for the installation of maintenance of all wireless equipment. No one else should install wireless equipment besides the ITS Networking personnel. Networking is also responsible for keeping an inventory of all equipment and documentation of security plans.

The Office of Cybersecurity is responsible for the auditing of the security plan and monitoring of traffic on the wireless networks.

Standard

1. 802.11x wireless networks must follow all requirements of Information Security Standards and Practices including, but not limited to, a risk assessment prior to implementation.
2. Security plan documentation must include, at a minimum, the department name, all AP locations, all supporting wireless infrastructure locations, the subnet on the wired network, and the Service Set Identifier (SSID).
3. APs and other supporting wireless devices must be placed in a physically protected location that minimizes opportunity for theft, damage or unauthorized access.
4. Wireless network coverage must be managed to restrict the ability to connect outside of the approved boundary.
5. The SSID of 802.11x wireless networks must be changed from the factory default setting.
6. The SSID must not include information that indicates the location, technology or manufacturer details of the wireless network (e.g., Server-Rm-WiFi-Access, Wifi-Rm70 and Cisco-2400-WiFi). The SSID also must not include information that indicates the type of data traversing the network.
7. Public wireless networks must be, at a minimum, physically separated from the internal network or configured to tunnel to a secure endpoint outside the internal network. The design must be included in the documented security plan.

8. Logical addressing schemas used for the wireless network must differ from those used for the wired network to effectively distinguish client connections between the two networks.
9. While servers and information stores may be accessible over a wireless network, they must not directly connect to a wireless network.
10. APs on public authenticated or internal wireless networks must be configured to provide the strongest encryption settings available. At a minimum, Wi-Fi Protected Access (WPA) 2 – Advanced Encryption Standard (AES) must be utilized.
11. WPA2 personal mode must not be used for internal networks.
12. WPA2 personal mode, with Wi-Fi Protected Access (WPS) disabled, may be used for public authenticated access points that do not connect to internal networks.
13. APs which utilize passphrases (such as APs configured to use WPA2 personal mode) must use passphrases that conform to AC-002.02-Password Management and Complexity.
14. Passphrases used by APs must be changed from the factory default setting.
15. The wireless network administration console must not be directly accessible from the wireless network.
16. 802.11x authentication, specifically the Extensible Authentication Protocol (EAP), must be used for all devices connecting to the internal wireless networks. SEs must use the EAP-TLS method whenever possible. Use of Lightweight EAP (LEAP) or use of the following EAP authentication mechanisms is not allowed: EAP-MD5 (Message Digest), EAP-OTP (One Time Password), and EAP-GTC (Generic Token Card).
17. Wireless client devices that connect to internal wireless networks must be configured to validate certificates issued by the authentication server during the authentication process.
18. Wireless client devices must be configured to utilize identity privacy settings during the authentication process, where technically feasible.
19. Individual user authentication, in accordance with AC-002-Authentication is required for internal wireless networks.

20. Exceptions to this Practice should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.

References

1. SC-001-Network Security
2. AC-002-Authentication
3. AC-002.02-Password Management and Complexity
4. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices