State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
143	B	Wireless Network 802.11x Installation, Configuration and Administration	08/01/2016	1 of 4

1.0 PURPOSE

This standard provides for the basic security of IEEE standard 802.11x wireless devices and methods used to establish data connections to or through such devices. This standard only addresses 802.11x wireless connectivity and does not discuss microwave communications.

2.0 SCOPE

This standard applies to any entity, regardless of physical location, that operates, manages or uses SilverNet services or equipment.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed agency Information Security Officer (ISO) have the responsibility to ensure compliance with this standard. It is the responsibility of the agency ISO or designee to provide oversight within the agency for all wireless access used by that agency. Unit managers are ultimately responsible for access to the systems, delegation of administrative tasks and editing and disseminating this standard.

5.0 RELATED DOCUMENTS

EITS Standard 117, Network Security Management
EITS Standard 119, Network Access Control

6.0 STANDARD

A. Before wireless access is connected to any Silvernet network, directly or indirectly, an approved Wireless Request must be received and processed by the ISO of the agency implementing the wireless access.

B. All wireless communications shall be encrypted and password protected.

C. Access points and bridges shall be connected to protected ports on a Local Area Network (LAN) switch or router using port security based on MAC address or 802.1x.

D. Antenna orientations and radiation strength should be set to minimize exposure outside of the areas of intended use.

E. Agencies should coordinate with residents of any adjacent structure within the signal coverage area to ensure radio interference does not occur.

F. The agency ISO or designee shall provide the Office of Information Security with an annual report identifying wireless devices in use by the agency. OIS will audit those devices on an annual basis.

G. Equipment must meet all applicable rules of regulatory agencies as established by the Federal Communications Commission (FCC). Vendor equipment is generally marked as certified for WiFi use.

H. Wireless access points and bridges must use secure administrative access control and protocols, such as IP specific administration restrictions or other methods as appropriate as well as SSL/TLS session encryption.

I. Wireless nodes or access points will be required to use one of the following Wi-Fi security methods:

   a. WPA + TKIP
   b. WPA + AES
   c. WPA2 + AES
   d. 802.11i

J. All wireless equipment will be compliant with IEEE 802.11x.

K. Abuse, interference or disruption of authorized communications shall be reported to the Office of Information Security (OIS).

L. A separate network authentication, authorization and accounting process must be used prior to allowing authorized wireless access points, bridges or clients access to Silvernet hosts. The authorization database cannot reside on the gateway between the wired and the wireless network and must reside within the wired network. Wireless client accounts cannot be maintained or managed on the wireless access point or bridge.

7.0 DEFINITIONS/BACKGROUND

802.11a – An IEEE specification for wireless networking in the 5GHz frequency range with a maximum 54Mbps data transfer rate. The 802.11a specification also includes Quality of Service (QoS) technology to protect voice and multimedia data.

802.11b – International standard networking technology for LAN wireless implementation that revised 802.11 to increase transmission speeds to 11Mbps.

802.11g – 802.11g will broaden 802.11b's data rates to 54Mbps within the 2.4 GHz band using Orthogonal frequency division multiplexing (OFDM).

802.11i – 802.11i is the IEEE standard for security in a wireless local area network.

802.11i – 802.11n operates on both the 2.4 GHz and lesser-used 5 GHz bands. It operates at a maximum net data rate from 54 Mbit/s to 600 Mbit/s.

Access Point (AP) – Wireless LAN transmitter/receiver that acts as a connection between wireless clients and wired networks.

Internal (network) – A state administered network not available by default to the general public.

Microwave – Frequencies ranging from 0.3 GHz to 300 GHz. Most applications are from 1.0 GHz to 40 GHz. Unlicensed point-to-point applications are typically in the 0.9 GHz, 2.4 GHz, 5.3 GHz, 5.8 GHz, and 60 GHz frequency range; while licensed point-to-point applications are typically 4.9 GHz and above. Some microwave uses are connectivity between buildings, leased line replacement, a cost effective alternative to fiber optics, and backhaul of data, voice and video. All State agencies must utilize EITS services except as otherwise provided for in NRS 242.131. Any State agency requiring microwave services must make a request to EITS Network Transport Services Manager utilizing the EITS Help Desk.

PKI - An acronym for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI or even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread.

SSID – Short for service set identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect.

VPN (Virtual Private Network) – A private data network that uses public telecommunications infrastructure while preserving privacy by using a tunneling protocol and other security measures. Using a VPN consists of encrypting information before sending it through the public network and then decrypting it at the other end. Companies have recently begun to consider using VPN to fulfill both their Intranet and Extranet needs.

Wireless – For the purpose of this standard, the IEEE 802.11x standards.

WPA (Wi-Fi Protected Access) – A specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is derived from and will be forward compatible with the upcoming IEEE 802.11i standard.

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
143	B	Wireless Network 802.11x Installation, Configuration and Administration	08/01/2016	4 of 4

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	7/28/2016
State Chief Information Security Officer (CISO)	Signature on File	7/28/2016
State Chief Information Officer (CIO)	Signature on File	8/1/2016

Document History		
Revision	**Date**	**Change**
A	05/01/16	Initial Release – Formerly EITS Standard 131
B	09/29/16	Minor changes to Section 6.0