SWAEC Wireless Security

All configuration parameters (such as Service Set Identifier (SSID), keys, passwords, etc.) of Wi-Fi access points or bridges that can be changed from default manufacturer settings shall be changed from the default and should be complex.

SWAEC offers open limited wireless networks. Public/guest wireless is limited to web traffic only. This service is provided to patrons and students in the surrounding area in order for them to access online coursework from the parking lots from which SWAEC is accessible.

Users of the SWAEC wireless network requiring access to systems or applications which contain data which is classified by the SS-70-70-001 Data and System Security Classification Standard as being Level B – Sensitive, Level C – Very Sensitive or Level D – Extremely Sensitive have appropriate access controls (firewall rules, router access control lists, and similar measures) that disallow wireless users from directly accessing the system or application. Users must use appropriate technology such as encrypted VPN, SSL/TLS, encrypted web pages, or similar authenticated and encrypted technologies to access these resources. This is in accordance to SS-70-009 Remote Access Standard and the SS-70-006 Encryption Standard. Examples include, but are not limited to: VPN, Routed traffic via the APSCN computer network, SSL connectivity to ADE resources, etc.

The daily operational SWAEC SSID must not contain information relative to agency location, mission, or name. SWAEC may temporarily employ the use of identifying SSIDs for the purposes of providing connectivity for training and/or limited access use.

SWAEC Wi-Fi equipment shall be configured for infrastructure mode only.

All wireless transmissions between SWAEC managed wireless access points or bridges and clients shall be encrypted utilizing the WPA protocol at a minimum to prevent unauthorized access to the state network. WEP (wireless encryption protocol) shall NOT be utilized due to its multiple security flaws.

Wirelessly transmitted data and credentials granting access to state resources are subject to the SS-70-009 Remote Access Standard and the SS-70-006 Encryption Standard.

SWAEC searches for and disables rogue Wi-Fi access points to the state network at least quarterly.

Wireless networks (Including Bluetooth, Wi-Fi, etc.) that covered entities may use that are separate from the state network are not subject to this standard. Clients however must still adhere to the SS-70-009 Remote Access Standard and the SS-70-006 Encryption Standard when accessing Level B, C, or D data from these outside environments.

Bluetooth wireless devices must be secured to the extent configurable between the devices involved and Bluetooth devices accessing SWAEC's network should follow the SS-70-009 Remote Access standard and the SS-70-006 Encryption standard.

Glossary

Bluetooth A computing and telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection.

Rogue Access Point Unauthorized wireless device allowing access to the state network

SSID (Service Set Identifier) A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.

State Network The state core information technology infrastructure serving Arkansas agencies, boards, commission, public schools, institutions of higher education, libraries, and other public organizations with Internet connectivity, data processing and transmission, video conferencing and telecommunications.

WEP (Wired Equivalent Privacy)– WEP is an optional privacy protocol originally specified in the IEEE 802.11 (802.11 legacy) standard that is designed to provide a level of security and privacy comparable to what is usually expected of a wired LAN. Weakness in the design makes this protocol unsuitable for use in environments which must protect sensitive data.

Wi-Fi A term used to describe the underlying technology of wireless local area networks (WLAN) based on the IEEE 802.11 set of specifications and is used interchangeably with the term wireless. Wi-Fi refers to any individual standard or the collection of all standards within the 802.11 family such as 802.11a, 802.11b/g, 802.11i, or 802.11n.

Wireless Wireless LAN (local area network) data access technology including the following protocols: 802.11 series and Bluetooth that accesses state information technology resources

WLAN (wireless local area network) A communication system that enables mobile users to connect to a wired network through a wireless (radio) connection, often implemented as an extension to wired LAN. WLAN'S are typically found
within a small client node, dense locale (e.g. a campus or office building), or anywhere a traditional network cannot be deployed for logistical reasons.

WPA (Wi-Fi Protected Access) WPA is a security standard for users of computers equipped with Wi-Fi wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP and also provides user authentication.