Information Technology Executive Council (ITEC)

ITEC-9500-S

1.0 TITLE: Wireless Local Area Network Standard

1.0 Effective Date: June 20, 2023

1.1 Type of Action: New

2.0 PURPOSE: To define the ITEC 9500-P minimum standards and procedures.

3.0 ORGANIZATIONS AFFECTED: All Branches, Boards, Commissions, Departments, Divisions, and Agencies of state government, hereafter referred to as entities.

4.0 REFERENCES:

4.0 ITEC Policy 1200 – Acceptable Use of the Internet

4.1 ITEC Policy 4010 - Technical Architecture Compliance Requirements

4.2 ITEC Policy 7230 – Information Technology Enterprise Security Policy

4.3 ITEC Policy 7230A – Information Technology Security Standards

4.4 ITEC Policy 9500-P

4.5 OITS Telecommunication Installation Guidelines

4.6 Kansas Information Technology Architecture Compliance Waiver – Attachment A

4.7 ITEC 9500S -Attachment B - Wireless Infrastructure Inventory

5.0 DEFINITIONS:

5.1 Wireless Local Area Network (WLAN) - is a local area network (LAN) that user's access through a wireless connection. WLANs may connect directly to various enterprise networks in the State of Kansas, including the KANWIN network, or may connect indirectly via the Internet and Virtual Private Networks (VPN). The State of Kansas defines WLANs in the following categories:

5.1.1 Enterprise Network: WLAN that is owned and operated by the State of Kansas and is used by authenticated users to access internal and external information technology resources.

5.1.2 Guest Network: WLAN owned and operated by the State of Kansas to provide un-managed access to the Internet. This network should not be considered a secure enterprise network.

5.1.3 Internet of Things (IoT) Network: WLAN owned and operated by the State of Kansas to provide encrypted un-managed access to the Internet. This network should not be considered a secure enterprise network.

5.2 KITA: Kansas Information Technology Architecture describes the information systems infrastructure that supports applications used by the State.

5.3 Security Mechanisms: Software or hardware devices used to secure a network or computer system. Examples of security mechanisms include passwords, firewalls, antivirus software, virtual private networks, and encryption protocols.

5.4 Mobile Computing Device: Laptop computer, handheld computer, cellphone, or other portable computing device used for data communications and/or data storage.

5.5 OITS: Office of Information Technology Services

5.6 Authenticated Users: User authentication verifies the identity of a user attempting to gain access to a network or computing resource by authorizing a transfer of credentials during interactions on a network to confirm a user's authenticity.

5.7 Guest User: Unauthenticated user where no user credentials are required when the user attempts to gain access to a network or computing resource.

5.8 Authorized Personnel: Authorized personnel means a person approved or assigned by the State Entity to perform a specific type of duty or duties.

5.9 Internet of Things (IoT): Are physical objects such as vehicles, electronics and other items embedded with software, sensors, actuators, that communicate, sense, or interact with their internal states or the external environment via network connectivity.

5.10 Simple Network Management Protocol (SNMP): Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

6.0 PROCEDURES:

6.1 Statement of Responsibility

6.1.1 The Branch CITOs shall be the point of contact and responsible for ensuring the compliance and standards set forth in this standard regarding the acquisition, installation, and management of all WLANs.

6.1.1.1 The Branch CITOs may, under certain conditions, delegate responsibility for acquisition, installation, and management to the entity requesting WLAN service, provided the proposed WLAN solution conforms to the standards set forth in this standard.

6.1.1.2 To ensure interoperability stated in this policy, WLANs shall not be acquired or installed without prior approval.

6.1.1.2.1 OITS shall ensure interoperability for WLAN equipment or software installations on OITS managed WLANs.

6.1.1.2.2 For acquisition or installation of WLAN equipment or software installation on Entity managed WLANs, the responsibility for ensuring interoperability lie with the entity CIO or delegate.

6.2 Acquisition

6.2.1 To maintain interoperability across the Enterprise WLAN, acquisition of all WLAN hardware and software shall conform to the KITA.

6.2.1.1 Only WLAN hardware and software that aligns with the KITA shall be purchased and installed.

6.2.1.2 To connect any WLAN equipment to OITS-managed networks, it must be procured through the OITS department.

6.2.1.2.1 WLAN equipment purchased for other WLAN's must be approved by the Entity CIO or delegate.

6.2.1.2.2 WLAN equipment purchased for other WLAN's must be enterprise networking equipment and comply with standards identified in the KITA.

6.2.1.3 Any exceptions to the KITA guidelines for WLAN hardware and software must submit the KITA waiver form following the approval process outlined in ITEC Policy 4010.

6.2.1.3.1 The ITEC Policy 9500-S "Kansas Information Technology Architecture Waiver – Attachment A" must be submitted to the Chief Information Technology Architect or delegate for approval.

6.3 Installation

6.3.1 Installation of WLANs in State entities shall conform to the requirements of the KITA and OITS Telecommunication Installation Guidelines.

6.3.1.1 Authorized personnel or approved vendors must perform all WLAN equipment or software installations on OITS-managed WLANS.

6.3.1.2 All WLAN equipment or software installation on Entity managed WLANS must be approved by the Entity CIO or delegate.

6.4 Management and Monitoring

6.4.1 A software tool shall be in place for the management and monitoring of all Enterprise or Guest WLANs provided by the State of Kansas. This tool shall be established by the entity responsible for the installation and management of the WLAN. OITS will establish, operate, and maintain the tool for all OITS managed WLANs, and management tools installed at separate entities shall be approved by the Entity CIO or delegate.

6.4.1.1 The Management and Monitoring tool may vary according to Entity but must allow for inventory and security/firmware updates of all infrastructure devices on the respective Entity's WLANs.

6.4.1.2 The Management and Monitoring tool installed must be capable of monitoring the network activity of all devices attached to the respective Entity's WLANs, to ensure suspicious and or disruptive devices can be quickly identified and removed from the affected WLAN in a prompt manner.

6.4.1.3 Management and Monitoring tool installed must be capable of signal strength, frequency, and performance metrics monitoring.

6.5 Security

6.5.1 Information transmitted over WLANs is inherently insecure. At a minimum, entity security policies for wireless communication devices used to access WLANs shall comply with this document and the KITA.

6.5.2 Wireless transmissions used to access enterprise networks shall be encrypted based on the specifications listed in KITA. All information is to be encrypted using the strongest and most cost-effective encryption available.

6.5.3 The Entity responsible for management of a WLAN shall maintain an inventory of authorized wireless access points and WLAN controllers. This inventory should include IP addresses, serial numbers, MAC address, device names, versioning, end of life information, and locations along with related technical diagrams. Refer to the ITEC Policy 9500-S Attachment B for a template.

6.5.4 User Security - user access to enterprise wireless networks shall be restricted to entity authorized personnel and should be maintained by entity authentication system.

6.5.4.1 User authentication will be maintained by the entities network access controls following the principle of least privilege.

6.5.4.2 Existing entity security policies will be followed for user password and authentication. Policies are: Wireless Local Area Network Policy - ITEC-9500-P, and KITA.

6.5.4.2.1 To meet the stated security goals of confidentiality, integrity, and availability, the State of Kansas will implement security mechanisms for wireless access to enterprise networks, including IEEE 802.1x authentication and the strongest and most cost-effective means encryption.

6.5.4.2.2 Segregation shall exist between entity guest and enterprise WLANs. Entity wired networks, using virtual LANs and entity firewalls, shall be used to segregate and support network access lists and traffic metering.

6.5.4.2.3 Implementing intrusion detection or prevention on entity firewalls and wireless systems is recommended but not required. This will assist in detecting and preventing:

- unauthorized users and access points from connecting to the network,
- denial of service,
- network layer attacks, and
- intercepting wireless transmission of authorized users.

6.5.4.2.4 Single sign-on capability is required using authentication methods, such as Windows Policy Server or supported Radius solution leveraging an existing authentication system.

6.5.4.2.5 Client devices shall not be allowed to "dual connect" where a device is connected to WLAN and the entity's LAN concurrently.

6.5.4.2.6 Entities who provide authentication to enterprise WLANs shall log access, including but not limited to, authentication attempts. The logs shall be retained according to the entity's log compliance requirements.

6.5.4.2.7 All vendor default passwords for wireless devices including Simple Network Management Protocol (SNMP) strings shall be changed prior to moving equipment into the production network.

6.6 Acceptable Use

6.6.1 Each entity is responsible for ensuring that the use of WLANs by authenticated users and guest users conform with statewide or entity WLAN policies regarding acceptable use of the KANWIN network, Internet (ITEC policy 1200), and entity enterprise networks per ITEC policy 7230 and 7230A.

6.6.1.1 Entities are responsible for establishing and maintaining network access policies for WLANs that are consistent with established security policy regarding user logons, passwords, and other relevant security mechanisms.

6.6.1.2 Guest Networks: To provide WLAN based Internet access to guests and visitors in a manner that protects the information technology assets of the State.

All guest networks must use an "acceptable use agreement" by utilizing a disclaimer page. A lease of the disclaimer page will be set when a user first authenticates for a period of no more than 24 hours total and no less than 60 minutes of idle time. Once the disclaimer has been accepted, it will not be prompted again until the idle timeout or the user has exceeded 24 hours in one session.

EXAMPLE: TERMS OF SERVICE

Accessing The (Entity) Public Network from Your Wireless Device – (Entity) provides Internet access at no charge in selected areas for guests with portable computers or devices capable of receiving wireless signals. To access the Internet from your wireless device, you must be sitting within range of a wireless access point. Guests are expected to use the wireless access in a legal and responsible manner. By using this wireless access network, you acknowledge that you are subject to, and agree to abide by, all laws and all state and federal rules and regulations applicable to Internet use and your use of this service.

Guests will need a mobile device equipped with a wireless access card that supports the WLAN standard.

You acknowledge that the (Entity) may disable or terminate your guest account for any reason without notice, for example, if problems originating from this account are detected.

Security Considerations - Anyone using the (Entity) wireless network is forewarned that there can be no expectation of privacy when using the wireless network. Wireless access is by nature an insecure medium. As with most guest wireless networks, any information being sent or received over the (Entity) wireless network could potentially be intercepted. Guests should not transmit their credit card information, passwords or any other sensitive information while using a WLAN.

You assume all risks associated with the use of this service. You agree to hold harmless the (Entity), its employees, and agents for any restricted use information (e.g. credit card) that is compromised, or for any damage caused to hardware or software due to electric surges, security issues or consequences caused by viruses or hacking. All guests should have up-to-date virus protection on their personal laptop computers or wireless devices, as well as up-to-date applicable OS security patches.

Disclaimer - The (Entity) is providing wireless connectivity in this facility as a guest service and offers no assurance or guarantee that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of this wireless connection is entirely at your own risk, and the (Entity) is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury, or damages resulting from the use of the wireless connection.

Agreement - By clicking "Accept" below, you agree to be bound by the above Terms of Service.

6.7 Internet of Things

6.7.1.1 Entities shall monitor these devices regularly for any potential security threats and ensure that they are regularly updated with the latest security patches.

6.7.1.2 Compliance with policies: All IoT implementations and associated data streams shall comply with ITEC Policy 7230, ITEC Policy 1200, and ITEC Policy 8010. It is important to understand and follow these policies to ensure the security and privacy of IoT devices and data.

6.7.1.3 Segregated network segment: IoT devices should be connected to a segregated network segment where costs are commensurate with risk and value, determined by the entity’s security office. This ensures that IoT devices are isolated from other network devices and prevents unauthorized access.

6.7.1.4 Encryption: All IoT device data transmitted or received should be encrypted. This ensures that data is protected in transit and prevents unauthorized access to the data. Refer to the KITA for encryption protocol standards.

6.7.1.5 When applicable change default Admin username and Password

6.7.1.6 Wireless network monitoring: All state-managed wireless networks shall be monitored to identify irregular traffic. This helps detect any unauthorized access or usage of IoT devices and prevents potential security threats.

6.7.1.7 Unauthorized IoT device detection: State entities shall have the ability to detect, isolate and remove unauthorized IoT devices. This helps prevent potential security threats from unauthorized devices that may have access to the network.

6.8 Network Usage

6.8.1 Access, authorization, and authentication to entity networks and IT resources via the WLAN shall be controlled by the respective State entity.

6.8.1.1 Access to the Enterprise WLAN is based on approval of overall network access.

6.8.1.2 Entities must conform to encryption standards defined in the KITA.

6.8.1.3 If entities are offering a Guest WLAN; entity may limit the maximum throughput for this network.

6.9 Asset Management

6.9.1 All State-owned wireless infrastructure components (e.g. wireless controllers, access points, wireless software, etc.) that provide connectivity to any wireless device, whether State or privately owned, shall be accounted for in the respective inventory system of the entity that is responsible for the installation, operation, and maintenance of that component.

6.9.2 Entities with components that attach the enterprise wireless network shall notify the entity that is responsible for the installation, operation, and maintenance of the WLAN.

7.0 RESPONSIBILITIES:

7.1 Heads of entities are responsible for establishing procedures for their organization's compliance with the requirements of this policy.

7.2 The Chief Information Technology Officer, Executive Branch, is responsible for the maintenance of this policy.

8.0 CANCELLATION: There are no previous versions of this standard.

9.0 HISTORY: Standard was implemented on June 20, 2023.