Information Technology Executive Council (ITEC)
ITEC-9500-P

1.0 TITLE: Wireless Local Area Network Policy

1.1 EFFECTIVE DATE: June 20, 2023

1.2 TYPE OF ACTION: Revised

2.0 PURPOSE: To establish a common, uniform use policy for all state agencies regarding the acquisition, installation, management, and use of Wireless Local Area Networks (WLAN) for use by authenticated users, and guest users.

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

4.0 REFERENCES:

4.1 K.S.A 75-4709 states that the Executive Chief Information Technology Officer (CITO) shall provide for and coordinate all telecommunications services for all divisions, departments, and agencies of the state pursuant to policies established by the Information Technology Executive Council (ITEC).

4.2 K.S.A. 75-7203(a) authorizes the ITEC to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state agencies.

4.3 K.S.A. 75-7221 - 75-7227 authorizes the Kansas Board of Regents for the creation, operation, and maintenance of the Kan-ed network.

4.4 ITEC Policy 1200 – Acceptable Use of the Internet

4.5 ITEC Policy 4010 - Technical Architecture Compliance Requirements

4.6 ITEC Policy 7230 - Information Technology Enterprise Security Policy

4.7 ITEC Policy 7230A – Information Technology Security Standards

4.8 ITEC Policy 8010A – Kansas Data Compliance Requirements

4.9 Kansas Information Technology Architecture Compliance Waiver – Attachment A

4.10 ITEC Policy 9500-S - Wireless Infrastructure Inventory - Attachment B

5.0 DEFINITIONS:

5.1 A Wireless Local Area Network (WLAN) is a type of Local Area Network (LAN) that allows wireless communication between devices within a limited geographical area, such as a home, office building, or campus. WLANs use the IEEE 802.11 standard to transmit data between devices, such as laptops, smartphones, and printers, using radio waves instead of physical cables. WLANs can connect directly to enterprise networks in the State of Kansas or indirectly via the Internet and Virtual Private Networks (VPN). The State of Kansas categorizes WLANs in the following categories:

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

5.1.2 Guest Network: a 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: a laptop computer, handheld computer, cellular phone, or other portable computing device used for data communications and/or data storage.

5.5 Personal Computing Device: any computing device that is not owned by the state.

5.6 Academic Network: a network designed to maintain free and open access to information which is not sensitive, and which is intended to be available to the public (Internet resources) or to the local campus community.

5.7 OITS: Office of Information Technology Services

5.8 Authenticated Users: are user credentials that are validated when the user attempts to gain access to a network or computing resource.

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

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

5.11 Internet of Things (IoT): 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.

6.0 POLICY: To establish a common, uniform policy for all entities regarding the acquisition, installation, management, and use of wireless local area networks, the following WLAN policies are established. This policy shall be the governing document for all entities WLAN policy. Any entity shall have the right to make additional restrictions to their own policy, but their policy shall not alter any provisions set forth in this policy.

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 policy 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 policy.

6.1.1.2 To ensure interoperability stated in this policy, WLANs shall not be acquired or installed without prior approval from the Branch CITOs or the Branch CITO's 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.

6.2.2 Waivers to the KITA for WLAN hardware and software shall be approved under the guidelines specified in ITEC 4010-P. Refer to Kansas Information Technology Architecture Compliance Waiver – Attachment A

6.3 Installation

6.3.1 Only WLAN hardware and software that aligns with the Technical Architecture of KITA shall be installed.

6.3.2 Only authorized personnel may install or add WLAN hardware and software.

6.3.3 A minimum of one enterprise and one public network should be implemented. Public Networks are designated for the public to gain access to the Internet. This public network should be isolated from the Enterprise network.

6.3.4 At least one enterprise wireless network is reserved for internal use by State entities. These networks are exclusively available to authenticated users and state managed devices.

6.4 Management and Monitoring

6.4.1 State entities deploying WLANs shall have responsibility and authority to implement WLAN management and monitoring capabilities.

6.4.1.1 OITS is responsible for overseeing and managing the State WLAN networks that they implement and support. Entities utilizing non-OITS managed WLANs may opt to add supplementary capabilities to improve the level of support for their WLAN networks.

6.4.2 State organizations are required to establish a protocol that enables them to identify the presence of any unauthorized wireless access points and to have a response procedure in place in the event such an access point is detected.

6.4.2.1 Any unapproved access point discovered in operation is subject to being disabled and/or removed immediately and permanently by the State entity or authorized personnel.

6.4.3 The State entity or authorized personnel shall relocate or remove any device or equipment found to be interfering with wireless access points within the premises of state-managed properties.

6.4.4 New Network Usage - access, authorization, and authentication to entity networks and IT resources via the WLAN shall be controlled by respective State entities responsible for that network.

6.5 Security

6.5.1 Information transmitted over WLANs is inherently insecure. At a minimum, wireless network security standards shall comply with ITEC-9500-S and the Wireless Networks section of the KITA.

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

6.5.3 The purchasing entity is responsible for maintaining an inventory of authorized wireless access points. For a description of inventory requirements, see ITEC-9500-S - Attachment B - Wireless Infrastructure Inventory.

6.6 Acceptable Use

6.6.1 It is the responsibility of each entity to ensure that authenticated users and guest users are aware of applicable acceptable use policies with either the statewide WLAN policy or the entity-specific WLAN policy with regard to the appropriate use of WLANs, the Internet (in accordance with ITEC policy 1200), and the entity's enterprise networks (in accordance with ITEC policies 7230 and 7230A).

6.6.1.1 To offer WLAN-based Internet access to guests and visitors in State-managed properties while safeguarding the State's information technology assets, a WLAN Guest network may be established to provide non-State personnel with access to the Internet. All guest networks must use an “acceptable use agreement” by use of a disclaimer page. See ITEC 9500-S.

6.6.1.2 When using the State's Enterprise WLAN or Guest WLAN, this policy requires all traffic transmitted and received to be encrypted.

6.6.1.3 Entities are accountable for creating and upholding network access policies for WLANs that align with the established security policy concerning security mechanisms such as user logons, passwords, and other relevant factors. Refer to ITEC 7230A.

6.6.2 Use of personal computing devices: Entities must ensure that employees using personal computing devices, on Enterprise WLANs comply with the security requirements and standards outlined in this policy.

6.6.3 Regents Universities may implement academic or research networks with or without authentication protocols with the approval of the heads of the respective university through university policy.

6.6.4 Regents Universities students, faculty, staff, and campus visitors may access academic networks with their personal wireless devices if those devices meet the same security standards required of state-owned devices.

6.7 Internet of Things (IoT)

6.7.1 State of Kansas classifies IoT into the following groups:

6.7.1.1 Administrative (i.e., state entity-owned and managed devices, contracted services)

6.7.1.2 Building management systems (e.g., specialized instruments, HVAC, elevators)

6.7.1.3 Community devices owned and operated by staff (e.g., televisions, Apple TV®, Chromecast™)

6.7.1.4 Research related IoT devices

6.7.1.5 Public-owned devices on the guest network

6.7.2 To connect an IoT device or group of devices to the states enterprise network, it is necessary to submit a written approval request to the entity head in accordance with the policy of the state entities.

6.7.3 If an IoT device causes disruption or security concerns with a state-managed enterprise network, the network manager or their delegate has the authority to remove that device.

6.7.4 For IoT device or collection of devices connecting to a guest network, any IoT device that causes disruption or security concerns with a state-managed guest network, the network manager or delegate has the authority to remove that device.

6.7.5 For IoT device or collection of devices connecting to an academic network, any IoT device that causes disruption or security concerns with a state-managed research network, the network manager or delegate has the authority to remove that device.

6.7.6 If a Building IoT device is connected to a state-managed network, and it poses a security risk or causes disturbance, the network manager or delegate is authorized to remove the device.

6.7.7 If a Community IoT device is connected to a state-managed network, and it poses a security risk or causes disturbance, the network manager or delegate is authorized to remove the device.

6.7.8 IoT devices connecting to enterprise networks shall have a process for updating software or firmware.

6.7.9 IoT Connectivity and Interoperability - for connectivity and interoperability standards, refer to KITA, Section IoT Network Protocols.

6.7.10 IoT Privacy and Security

6.7.10.1 Each IoT implementation and associated data streams shall comply with ITEC Policy 7230, ITEC Policy 1200, and ITEC Policy 8010.

6.7.10.2 IoT devices should be connected to a segregated network segment where costs are commensurate with risk and value, determined by the entity's IT security office. All IoT device data transmitted or received should be encrypted.

6.7.10.3 All state-managed wireless networks shall be monitored to identify irregular traffic. State entities shall have the ability to detect, isolate and remove unauthorized IoT devices.

6.8 Asset Management

6.8.1 All State-owned wireless infrastructure components (i.e., 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. Refer to ITEC Policy 9500-S - Wireless Infrastructure Inventory - Attachment B

6.8.2 Entities with mobile or personal computing devices that attach to the enterprise WLAN 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 to establish procedures for their organizations to comply 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: All previous versions of this policy.

9.0 HISTORY: Policy was implemented on April 27, 2006, and updated on June 20, 2023.