7-105. Wireless local area network standard.

(1) Purpose. The purpose of this standard is to ensure that only properly secured and managed wireless local area networks are deployed by state agencies.

(2) Registration Requirement. All wireless local area networks that connect to the state network must be registered with the Office of the CIO.

(3) Registration Process. The registration process will identify: contact information; device information, including the manufacturer, model, and physical location; the security/firewall technologies being deployed; where logging information is to be stored; and, if the use of the wireless access is only for internet, a description showing how traffic will be separated. Registration information must be submitted to the Office of the CIO Service Desk. Registration must occur prior to deployment. The Office of the CIO will contact the registering agency after reviewing the registration information. Final device names are assigned by the Office of the CIO during the registration process to avoid conflicts and confusion, and to aid in incident response and in identifying and locating wireless devices. If technology allows for the broadcast of a device name, standardized names should appear in the broadcast description, along with any unique identifiers assigned to the unit.

(4) Unregistered and Unsecured Devices. Only approved wireless local area networks and access points will be deployed within state agencies. Unregistered devices will be removed from service. Network managers for the Office of the CIO will incorporate procedures for scanning for unregistered wireless devices and access points. The Office of the CIO may disable network access for a device, server or network if inadequate security is found or improper procedures are discovered.

(5) Management and Security of Access Points.

(a) Physical Security. Access points must be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices must not be placed in easily accessible public locations.

(b) Configuration Management. All wireless access points must be secured using a strong password. Passwords must be changed at least every six months. Administrators must ensure all vendor default user names and passwords are removed from the device.

(6) Security of the Wireless Network.

(a) Logging. All access to the wireless network must be logged with records kept for a minimum of one year. Records must include the time of access, the IP and MAC addresses of the device, and the username.

(b) Access to the State Network. Accessing the state network requires a username and password combination that is unique to each user. The SSID must use a minimum of WPA2 with the use of a FIPS 140-2 validated AES encryption module.

(c) Wireless Intrusion Detection Systems. All wireless networks must use a wireless intrusion detection systems (WIDS) capable of location detection of both authorized and unauthorized wireless devices. All systems must provide continuous scanning and monitoring. WIDS logs and documented actions must be maintained for a minimum of one year

(7) Management of Airspace. All conflicts regarding wireless connectivity are resolved by the Office of the CIO.

--

History: Adopted on September 30, 2013. Renumbered on July 12, 2018 (previously was § 7-301). Amended on August 4, 2006; April 11, 2012; and July 12, 2018.
URL: http://nitc.nebraska.gov/standards/7-105.pdf