**State of Nebraska**
**Nebraska Information Technology Commission**
**Standards and Guidelines**

**NITC 7-301 (DRAFT REVISED)**

| | |
|---|---|
| Title | Wireless Local Area Network Standard |
| Category | Network Architecture |
| Applicability | Applies to all state agencies, boards, and commissions, excluding higher education |

## 1. Standard

This standard applies to state agencies which deploy a Wireless Local Area Network (WLAN). This standard is in replacement of previous requirements and is retroactive in perpetuity in the pursuit of remaining current with the constantly changing security needs of wireless connectivity.

### 1.1. Registration of Wireless Devices

State agencies must register WLANs, including each Access Point (AP) that connects to the State of Nebraska's private network, with the Office of the CIO (OCIO).

#### 1.1.1. Registration

The registration process will identify: contact information; WLAN device information, including the manufacturer, model, and physical location; the security/firewall technologies being deployed; and, where logging information is to be stored. Registration information should be submitted to the CIO Help Desk at [URL to be added]. **Registration must occur prior to deployment** to prevent the access point from being declared as rogue.

#### 1.1.2. Review and Approval

The OCIO will contact the registering agency after reviewing the registration information.

#### 1.1.3. Naming Convention

Final device names are assigned by the OCIO 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.

#### 1.1.4. Unregistered (Rogue) and Unsecured Devices

Only approved WLANs and access points will be deployed within state agencies. **Unregistered (rogue) devices will be removed from service.** Network managers for the OCIO will incorporate procedures for scanning for unregistered (rogue) wireless devices and access points. This requires a full understanding of

the topology of the network. It also requires performing periodic security testing and assessment, including randomly timed security audits to monitor and track wireless and handheld devices. **OCIO reserves the right to disable network access for a device, server or LAN if inadequate security is found or improper procedures are discovered.**

#### 1.1.5. Internet Only Wireless

If the use of the wireless access is only for internet, then the requesting agency must provide a written method showing how they plan on keeping traffic separate.

### 1.2. Management and Security of the access point

#### 1.2.1. Physical Security

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

#### 1.2.2. Configuration Management

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

### 1.3. Security of the wireless network

#### 1.3.1. Logging

All access to the wireless network must be logged with records kept for a minimum of one (1) year. Records must include the time of access, the IP and MAC addresses of the device, and the username.

#### 1.3.2. Access to State Network

If access is to the states network:

**1.3.2.1.** Access to the wireless network requires a username and password combination that is unique to each user; and

**1.3.2.2.** The SSID must use a minimum of WPA2 with the use of a FIPS 140-2 validated AES encryption module

#### 1.3.3. Wireless Intrusion Detection Systems

All wireless networks require the use of wireless intrusion detection systems (WIDS), capable of location detection of both authorized and unauthorized wireless devices. All systems will provide 24/7 continuous scanning and monitoring. WIDS logs and documented actions will be maintained for a minimum of (1) year.

### 1.4. Management of Airspace

All conflicts regarding wireless connectivity are resolved by the OCIO. Review of airspace requirements and changes will be addressed with notification of compliance.

## 2. Purpose

Wireless communications offer organizations and users many benefits such as portability, flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs.

In additional to the inherent risks associated with any wired network, wireless technology introduces several unique vulnerabilities. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk. These include correspondence, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks. Also, since wireless network devices operate using radio signals, their proliferation within an area can lead to Radio Frequency Interference (RFI) among these devices and other radio devices using the same frequency bands.

The purpose of this standard is to ensure that only properly secured and managed WLANs are deployed by agencies.

---
VERSION DATE: DRAFT - February 9, 2012.
REPEALER: Original NITC 7-301 is repealed.
HISTORY: Adopted on September 30, 2003. Revised on August 4, 2006.
PDF FORMAT: (to be added)
---