NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Wireless Local Area Network Guidelines

Category	**Security Architecture**
Title	**Wireless Local Area Network Guidelines**
Number	**XX-XXX**

Applicability

☑ **State Government Agencies**
- ☐ All.....**Not Applicable**
- ☑ Excluding higher education institutions.....**Standard (§1.1) and Guideline**

☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.....**Not Applicable**

☑ **Other:** All Public Entities.....**Guideline**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____.
Guideline - Adherence is voluntary.

Status	☐ Adopted	☑ Draft	☐ Other:_____
Dates	Date: August 13, 2003 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard and Guidelines

STANDARD (For state government agencies only, excluding higher education institutions.)

1.1 Registration of Wireless Devices

- Registration of access clients is not required unless the same device is configured as an access point.
- All wireless network access points should be registered with the network manager for that entity. State agencies must register Wireless Local Area Networks with IMServices. Self-registration will be available through the IMServices web site (www.ims.state.ne.us). The registration process will identify: a) the physical location of the network, b) the security/firewall technologies being deployed, and c) the types of services or information that is available through the wireless LAN. IMServices reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place. Wireless services that fall within the definition of campus connection, MAN or WAN must be purchased through the Division of Communications to comply with State statutes.
- Agencies using wireless systems must develop general risk mitigation strategies for access points, users and client devices such as virus protection, password standards, and other preventative measures.
- Only approved and registered access points will be deployed within state agencies. Unapproved (rogue) devices should be removed from service.

GUIDELINES

1.2 Management and Security of Access Points

- *Physical Security*: Access points should be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices should not be placed in easily accessible public locations.
- *Configuration Management*: All wireless access points should be secured using a strong password. Passwords should be changed at least every six months. Administrators should ensure all vendor default usernames and passwords are removed from the device. Administration of the device should be prohibited from the wireless network.
- *Rogue Wireless LANS*: Network managers for each entity should incorporate procedures for scanning and detecting 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.

1.3 Broadcast Security and Encryption

- Agencies deploying wireless technology should adhere to minimum encryption standards, and follow best practices for secure installations.

1.4 Access to Systems and Data

- Agencies and other entities connected to the state's network must employ adequate security to protect other systems and data connected to the state's network.
- Once authenticated to an access point, users should either be routed outside the state's firewall(s), or authenticated to the network. Just as with a wired network, state network authentication--whether enterprise-wide or agency-specific-- should satisfy prescribed login/password combinations prior to using enterprise or agency-specific resources that are not normally accessible by nodes outside the state's firewall(s).

- Access control mechanisms such as firewalls should be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks should employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

1.5 Naming Conventions

- Final device names are assigned 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.

1.6 Disruption and Interference

- All newly deployed wireless technologies should satisfy all existing and future standards as required by law or established by the NITC or the Information Management Services Division pertaining to use and security of the state's network.
- An entity's network manager should resolve any conflicts between wireless devices. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate. For state agencies, excluding higher educational institutions, IMServices will resolve any conflicts between wireless devices, in coordination with affected agencies.

2.0 Background

2.1 Purpose and Objectives

In some situations, wireless technology offers important advantages in terms of convenience, flexibility and cost savings over other types of networking. A major disadvantage of wireless technology is its inherent security risks. If not deployed properly, a wireless local area network (LAN) offers open access to everyone in the vicinity who has a wireless card in his or her PC, laptop, Personal Digital Assistant (PDA), wireless messaging devices or other computing devices.

The purpose of these guidelines is to encourage wise decisions regarding whether and how to implement wireless technology. The primary source of these guidelines is the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, which has issued Special Publication 800-48, "Wireless Network Security 800.11, Bluetooth and Handheld Devices," November 2002. A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

NIST Special Publication 800-48 is 119 pages long. It provides a detailed overview of wireless technology, wireless LANs, wireless personal area networks ("Bluetooth" technology), and wireless handheld devices. Anyone implementing any of these types of wireless systems should read the entire report, which is incorporated into these guidelines by reference. The following guidelines copy the executive summary and the checklist in NIST SP 800-48 that specifically pertain to wireless LANs. Parts of the Executive Summary and most of Section D are based on the National Institutes of Health Wireless Network Policy.

As a final cautionary note, the ease and convenience of setting up wireless LANs should not outweigh the responsibility of every agency to consider the "security needs of other agencies or institutions connected to the network".

In addition to following the NIST SP 800-48, any public entity implementing wireless technology should notify that entity's network manager before connecting the wireless device to the entity's network. State government agencies, excluding higher educational institutions, must comply with notification procedures established by the Division of Communications and the Information Management Services Division, as described in Section 1.1.

These general guidelines do not replace or supercede any specific standards and procedures of operational entities, which have responsibility for managing communications networks.

2.2 Executive Summary

Wireless communications offer organizations and users many benefits such as portability and 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. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

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, including 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, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

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.

This document provides an overview of wireless networking technologies and wireless handheld devices most commonly used in an office environment and with today's mobile workforce. This document seeks to assist agencies in reducing the risks associated with 802.11 wireless local area networks (LAN), Bluetooth wireless networks, and handheld devices.

These guidelines recommend the following actions:

1. Agencies should be aware that maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Moreover, it is important that agencies assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

2. Agencies should not undertake wireless deployment for essential operations until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations. Agencies should perform a risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products should be considered for purchase.

3. Agencies should be aware of the technical and security implications of wireless and handheld device technologies.

4. Agencies should carefully plan the deployment of 802.11, Bluetooth, or any other wireless technology.

5. Agencies should be aware that security management practices and controls are especially critical to maintaining and operating a secure wireless network.

6. Agencies should be aware that physical controls are especially important in a wireless environment.

7. Agencies should enable, use, and routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies.

8. In addition, firewalls and other appropriate protection mechanisms, such as intrusion detection systems should be employed.

3.0 Definitions

3.1 **Access Point**. A hub or interconnect device on a Local Area Network (LAN) that supports wireless (IEEE 802.11x) devices such as laptops, PDA's, etc. In some cases, the Access Point constitutes a stand-alone LAN where only a few wireless devices that need to communicate or share resources.

3.2 **Campus Connection**. (to be defined)

3.3 **Local Area Network (LAN)**. A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For State agencies, LANs are defined as restricted to rooms or buildings. An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN).

3.4 **Metropolitan Area Network (MAN)**. A data communications network that (a) covers an area larger than a local area network (LAN) and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

3.5 **Personal Digital Assistant (PDA)**. A handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, a to-do

list, and a note taker. PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data are synchronized between a user's PDA and desktop computer by cable or wireless transmission.

3.6 **Smart Card**. A credit card with a built-in microporcessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

3.7 **Virtual Private Network**. A means by which certain authorized individuals (such as remote employees) can gain secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

3.8 **Wide Area Network (WAN)**. A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide.

3.9 **Wireless Application Protocol (WAP)**. A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages.

3.10 **Wired Equivalent Privacy (WEP)**. Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

4.0 Applicability

These guidelines are intended to be useful to all public entities that are developing their own security policies and procedures for wireless networks. They specifically apply to state government agencies, excluding higher educational institutions.

5.0 Responsibility

5.1 **Agency and Institutional Heads**. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, including disaster recovery plans for information technology. The authority may delegate this responsibility but delegation does not remove the accountability.

5.2 **Agency Information Officer**. The Agency Information Officer or delegate must notify the Division of Communications and the Information Management Services Division before implementing a wireless system.

5.3 **Information Management Services Division (IMServices)**. IMServices shares responsibility with the Division of Communications for the security of the state's network. State agencies must register Wireless Local Area Networks with IMServices. Self-registration will be available through the IMServices web site (www.ims.state.ne.us). IMServices reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place.

5.4 **Division of Communications (DOC)**. DOC shares responsibility for the security of the state's network with IMServices. Wireless services that fall within the definition of campus

connection, MAN or WAN, must be purchased through the Division of Communications to comply with State statutes.

6.0 Related Policies, Standards and Guidelines

6.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)

6.2 NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)

6.3 NITC Incident Response and Reporting Procedures for State Government (http://www.nitc.state.ne.us/standards/index.html)

7.0 References

7.1 NIST Wireless Network Security Special Publication 800-48 (http://csrc.nist.gov/publications/nistpubs/index.html)

7.2 National Institutes of Health (NIH) Wireless Network Policy, January 24, 2003, (http://www1.od.nih.gov/oma/manualchapters/management/2807/)

7.3 Information Management Services Division, "Network Security Standards" (Draft, February 11, 2003), www.ims.state.ne.us.

APPENDIX

Wireless LAN Security Checklist

The table, below, provides a WLAN security checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network, based on NIST Special Publication 800-48. Most of the recommendations are "best practices", which all agencies should be followed. Items marked as "Should Consider" might provide a higher level of security, but should be weighed against other considerations.

Management Recommendations

Status	Recommendation
	1. Develop an agency security policy that addresses the use of wireless technology, including 802.11.
	2. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.
	3. Perform a risk assessment to understand the value of the assets in the agency that need protection.
	4. Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).
	5. Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.
	6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
	7. Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).
	8. Complete a site survey to measure and establish the AP coverage for the agency.
	9. Take a complete inventory of all APs and 802.11 wireless devices.
	10. Ensure that wireless networks are not used until they comply with the agency's and the state's security policies.
	11. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
	12. Place APs in secured areas to prevent unauthorized physical access and user manipulation.

Technical Recommendations

Status	Recommendation
	13. Empirically test AP range boundaries to determine the precise extent of the wireless coverage.
	14. Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).
	15. Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.
	16. Restore the APs to the latest security settings when the reset functions are used.
	17. Change the default SSID in the APs.
	18. Disable the broadcast SSID feature so that the client SSID must match that of the AP. (Should Consider)

	19. Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.
	20. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.
	21. Understand and make sure that all default parameters are changed.
	22. Disable all insecure and nonessential management protocols on the APs.
	23. Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.
	24. Ensure that encryption key sizes are at least 128-bits.
	25. Make sure that default shared keys are periodically replaced by more secure unique keys.
	26. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).
	27. Install antivirus software on all wireless clients.
	28. Install personal firewall software on all wireless clients.
	29. Disable file sharing on wireless clients (especially in untrusted environments).
	30. Deploy MAC access control lists. (Should Consider)
	31. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.
	32. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications. (Should Consider)
	33. Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.
	34. Fully test and deploy software patches and upgrades on a regular basis.
	35. Ensure that all APs have strong administrative passwords.
	36. Ensure that all passwords are being changed regularly.
	37. Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI. (Should Consider)
	38. Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
	39. Use static IP addressing on the network. (Should Consider)
	40. Disable DHCP. (Should Consider)
	41. Enable user authentication mechanisms for the management interfaces of the AP.
	42. Ensure that management traffic destined for APs is on a dedicated wired subnet.
	43. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.

Operational Recommendations

Status	Recommendation
	44. Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.
	45. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.
	46. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information. (Should Consider)

	47. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos. (Should Consider)
	48. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity. (Should Consider)
	49. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity. (Should Consider)
	50. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features. (Should Consider)
	51. Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.
	52. Fully understand the impacts of deploying any security feature or product prior to deployment.
	53. Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology. (Should Consider)
	54. Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features. (Should Consider)
	55. When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.
	56. If the access point supports logging, turn it on and review the logs on a regular basis.