Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Wireless Local Area Network 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. Items marked 'REQUIRED" must be fulfilled in order to meet the specifications of this standard. Items marked as "Strongly Advise" might provide a higher level of security, but should be weighed against other considerations.

Management

Status	Tasks
REQUIRED	1. Develop an agency security policy that addresses the use of wireless technology, including 802.11.
REQUIRED	2. Maintain a complete inventory of all APs and 802.11 wireless devices.
REQUIRED	3. Ensure that wireless networks are not used until they comply with the agency's and the state's security policies.
Strongly Advise	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).
Strongly Advise	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.
Strongly Advise	6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
Strongly Advise	7. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
Strongly Advise	8. Complete a site survey to measure and establish the AP coverage for the agency.
Strongly Advise	9. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.
Strongly Advise	10. Perform a risk assessment to understand the value of the assets in the agency that need protection.
Strongly Advise	11. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
Optional	12. Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).

Technical

Status	Tasks
REQUIRED	13. Change the default SSID in the APs
REQUIRED	14. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference
REQUIRED	15. Disable all insecure and nonessential management protocols on the APs.
REQUIRED	16. Enable all security features of the WLAN product, including the cryptographic authentication and privacy feature.
REQUIRED	17. Ensure that encryption key sizes are at least 128-bits.
REQUIRED	18. Install antivirus software on all wireless clients.
REQUIRED	19. Ensure that all managed APs have strong administrative passwords.
REQUIRED	20. Enable user authentication mechanisms for the management interfaces of the AP.
Strongly Advise	21. Empirically test AP range boundaries to determine the precise extent of the wireless coverage.
Strongly Advise	22. Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.
Strongly Advise	23. Restore the APs to the latest security settings when the reset functions are used.
Strongly Advise	24. Understand and make sure that all default parameters are changed.
Strongly Advise	25. Make sure that shared keys are periodically replaced by more secure unique keys.
Strongly Advise	26. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).
Strongly Advise	27. Install personal firewall software on all wireless clients.
Strongly Advise	28. Deploy MAC access control lists.
Strongly Advise	29. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.
Strongly Advise	30. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.
Strongly Advise	31. Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.
Strongly Advise	32. Fully test and deploy software patches and upgrades on a regular basis.
Strongly Advise	33. Ensure that all passwords are being changed regularly.
Strongly Advise	34. 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.
Strongly Advise	35. Ensure that management traffic destined for APs is on a dedicated wired subnet.
Strongly Advise	36. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
Optional	37. Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).
Optional	38. Disable the broadcast SSID feature so that the client SSID must match that of the AP.
Optional	39. Validate that the SSID character string does not reflect the agency’s name (division, department, street, etc.) or products.
Optional	40. Disable file sharing on wireless clients (especially in untrusted environments).
Optional	41. Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.

Optional	42. Use static IP addressing on the network
Optional	43. Disable DHCP.

Operational

Status	Tasks
REQUIRED	44. 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.
Strongly Advise	45. 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.
Strongly Advise	46. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.
Strongly Advise	47. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.
Strongly Advise	48. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.
Strongly Advise	49. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.
Strongly Advise	50. Fully understand the impacts of deploying any security feature or product prior to deployment.
Strongly Advise	51. 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.
Strongly Advise	52. If the access point supports logging, turn it on and review the logs on a regular basis.
Optional	53. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.
Optional	54. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.
Optional	55. Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct keys.
Optional	56. Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.