

## Wireless LAN Security Summary

Objectives:	Procedures	Status	Notes
1. Develop an agency security policy that addresses the use of wireless technology, including 802.11.	A security policy is the foundation on which other countermeasures—the operational and technical ones—are rationalized and implemented. A documented security policy allows an organization to define acceptable architecture, implementation, and uses for 802.11 wireless technologies.		
2. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (e.g., 802.11).	A security awareness program helps users to establish good security practices to prevent inadvertent or malicious intrusions into an organization's information systems.		
3. Perform a risk assessment to understand the value of the assets in the agency that need protection.	Understanding the value of organizational assets and the level of protection required is likely to enable more cost-effective wireless solutions that provide an appropriate level of security.		
4. Ensure that the client NIC and AP support firmware upgrades so that security patches may be deployed as they become available (prior to purchase).	Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.		
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.	Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it stays secure. Random checks ensure that the security posture is maintained beyond periods of assessment.		
6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	The external boundaries should be secured to prevent malicious physical access to an organization's information system infrastructure such as a fence or locked doors.		
7. Deploy physical access controls to the building and other secure areas (e.g., using photo IDs or card badge readers).	Identification badges or physical access cards help to ensure that only authorized personnel have access to gain entry to a facility.		
8. Complete a site survey to measure and establish the AP coverage for the agency.	Proper placement of Access Points will help ensure that there is adequate wireless coverage of the environment while minimizing exposure to external attack. The site survey should result in a report that proposes AP locations, determines coverage areas, and assigns radio channels to each AP and that ensures that the coverage range does not expose APs to potential malicious activities.		
9. Take a complete inventory of all APs and 802.11 wireless devices.	A complete inventory list of APs and 802.11 wireless devices can be referenced when conducting an audit for unauthorized use of wireless technologies.		
10. Ensure that wireless networks are not used until they comply with the agency's security policy.	Security policy enforcement is vital for ensuring that only authorized APs and 802.11 wireless devices are operating in compliance with the organization's wireless security policy.		
11. Locate APs on the interior of buildings instead of near exterior walls and windows.	Locating APs near exterior walls and windows provides a better range of access to potential external malicious users. Choosing the location wisely to balance security and coverage should be considered.		
12. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Physically securing the APs, putting them "out of reach," prevents unauthorized access by potential malicious users.		
13. Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	By empirically testing the AP coverage range for an agency, a level of risk associated with the access range by potential malicious users can be better understood.		

14. Make sure that APs are turned off while they are not being used (e.g., after hours, weekends).	Shutting down APs when not in use minimizes potential exposure to malicious activity.		
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.	The reset function allows an individual to negate any security settings administrators have configured on an access point.		
16. Restore the APs to the latest security settings when the reset functions are used.	Security settings are lost after a reset function. Therefore, the appropriate personnel should restore the latest security settings after a reset.		
17. Change the default SSID in the APs.	Many default SSIDs used by vendors are published and well known. Malicious users often try to connect to 802.11 networks using the default SSID.		
18. Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Malicious users can more easily detect and exploit APs that are broadcasting the SSID. Disabling the broadcast SSID feature minimizes exposure of the AP to malicious users.		
19. Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	The SSID should be somewhat difficult for malicious users to use to determine the organization or agency that owns the AP. The SSID should also be long and difficult to guess.		
20. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	Radio interference between APs can result in a denial of service. So, using channels in a different range ensures service availability.		
21. Understand and make sure that all default parameters are changed.	Because default settings are generally known and not secure, these settings should be changed and should comply with organizational security policy.		
22. Disable all insecure and nonessential management protocols on the APs.	Management protocols that are enabled on APs but not used present a potential avenue of attack. Disabling all insecure and nonessential management protocols minimizes potential methods that a hostile entity can use when attempting to compromise an access point.		
23. Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy features.	Enabling built-in security features provides greater security than the default settings.		
24. Ensure that encryption key sizes are at least 128 bits or as large as possible.	Brute force attacks on encryption key sizes become more difficult as the key sizes increase. The addition of a single bit doubles the key space. A 128-bit provides an "intractable" key space against cryptanalysis, if the algorithm and implementation are sound.		
25. Make sure that default shared keys are periodically replaced by more secure unique keys.	Changing default shared keys periodically decreases the likelihood that a malicious user can exploit a compromised key. A changed key increases the adversary's difficulty.		
26. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	A firewall can enforce a security policy on the information flow between the wired network and the wireless network.		
27. Install antivirus software on all wireless clients.	Antivirus software helps ensure that the wireless client does not introduce known worms and viruses to the wired network while protecting the wireless client from viruses that originate on the wired network.		
28. Install personal firewall software on all wireless clients.	Personal firewalls help to protect against wireless network attacks.		
29. Disable file sharing on wireless clients (especially in untrusted environments).	Malicious users can potentially exploit wireless clients enabled for file sharing.		
30. Deploy MAC access control lists.	The use of access control lists based on MAC hardware addresses provides a layer of security that ensures that only authorized wireless devices are allowed to connect to the wired network.		

31. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	The use of layer 2 switches segments network traffic and minimizes potential for a hostile user to monitor traffic by connecting to a hub.		
32. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.	The use of IPsec-based VPN provides an overlay protection to the standard link encryption (e.g., WEP) provided by the wireless connecting hosts.		
33. Ensure that encryption being used is sufficient with the sensitivity of the data on the network and the processor speeds of the computers.	Sensitive data transmission should be encrypted. The level of encryption provided must be balanced between data security requirement and overhead cost related to processor capability.		
34. Fully test and deploy software patches and upgrades regularly.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should also be fully tested before implementation to ensure that they work.		
35. Ensure that all APs have strong administrative passwords.	Administrator passwords on APs should not be easy to guess. This minimizes the risk of an unauthorized user gaining access by guessing or cracking administrative passwords.		
36. Ensure that all passwords are being changed regularly.	Passwords should changed regularly to reduce the risk of a compromised password being exploited.		
37. Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.	Implementing strong or two-factor authentication whenever possible minimizes the vulnerabilities associated with simple username and password authentication.		
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 a different vendor. The "ad hoc mode" for 802.11 can be exploited. Users of hosts with "ad hoc mode" enabled may unintentionally allow users to inadvertently or maliciously connect to those systems.		
39. Use static IP addressing on the network.	Using static IP addressing makes it more difficult for a hostile user to connect to the network.		
40. Disable DHCP.	If DHCP is disabled, then hosts are forced to use a static IP address.		
41. Enable user authentication mechanisms for the management interfaces of the AP.	User authentication mechanisms should be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP.		
42. Ensure that management traffic that is destined for APs is on a dedicated wired subnet.	Passing management traffic over an "out of band" network or management subnet protects management traffic, interfaces, and passwords from organizational and outside users.		
43. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.	SNMPv3 has enhanced security features relative to its predecessor SNMP protocol. SNMPv3 and SSL/TLS provide for secure authentication and encryption for Web-based management access of APs.		
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. Company that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and so are fundamentally insecure and not recommended. Agencies should use SNMPv3.		
45. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	AP management traffic should be cryptographically protected. SNMPv3 provides cryptographic mechanisms to provide strong security.		
46. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.	By using a local serial port interface for AP configuration ensures that sensitive management information do not traverse the network as well as minimizing the risk of unauthorized users gaining access via a network protocol used to manage the AP.		

47. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.	Use of authentication mechanisms such as RADIUS and Kerberos can improve the security and simplify user management.		
48. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.	Intrusion detection agents (e.g., host-based or networkbased agents) deployed on the wireless network can detect and respond to potential malicious activities.		
49. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.	If RADIUS is used, the audit records should be manually or automatically processed to determine if malicious activity has been directed at the authentication server.		
50. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.	During product selection, ensure that the product provides enhanced cryptographic protection or user authorization features.		
51. Enable use key-mapping keys rather than default keys so that sessions use distinct WEP keys.	The use of distinct WEP keys provides more security than default keys and reduces the risk of key compromise.		
52. Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements before implementation.		
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.	An appointed individual designated to track the latest technology enhancements, standards, and risks will help to ensure the continued secure implementation of wireless technology.		
54. Wait for future releases of 802.11 WLAN technologies that incorporate fixes to the security features, or provide enhanced security features.	Upgrade to the latest versions and avoid purchasing the versions of the 802.11 products with major security vulnerabilities that have not been fixed.		
55. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Sensitive or proprietary configuration settings should be cleared from access points before removing them from use or disposing to prevent inadvertent disclosure of the information to potentially malicious users.		
56. If the access point supports logging, turn it on and review the logs on a regular basis.	Ensure that the APs are set to perform logging. Also, review of audit and logging data helps to ensure user accountability.		
57. If the access point supports logging, turn it on and review the logs on a regular basis.	Access point logs should be enabled and regularly reviewed for malicious activity.		