

ISO 27001 Wireless LAN Security Checklist

No	Type	Procedures	Status	Notes
1	Management Recommendations	Develop an agency security policy that addresses the use of wireless technology, including 802.11.		
2	Management Recommendations	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.		
3	Management Recommendations	Perform a risk assessment to understand the value of the assets in the agency that need protection.		
4	Management Recommendations	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	Management Recommendations	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	Management Recommendations	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.		
7	Management Recommendations	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).		
8	Management Recommendations	Complete a site survey to measure and establish the AP coverage for the agency.		
9	Management Recommendations	Take a complete inventory of all APs and 802.11 wireless devices.		
10	Management Recommendations	Ensure that wireless networks are not used until they comply with the agency's security policy.		
11	Management Recommendations	Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.		
12	Management Recommendations	Place APs in secured areas to prevent unauthorized physical access and user manipulation.		
13	Technical Recommendations	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.		
14	Technical Recommendations	Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).		
15	Technical Recommendations	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	Technical Recommendations	Restore the APs to the latest security settings when the reset functions are used.		
17	Technical Recommendations	Change the default SSID in the APs.		
18	Technical Recommendations	Disable the broadcast SSID feature so that the client SSID must match that of the AP.		
19	Technical Recommendations	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.		
20	Technical Recommendations	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.		
21	Technical Recommendations	Understand and make sure that all default parameters are changed.		
22	Technical Recommendations	Disable all insecure and nonessential management protocols on the APs.		
23	Technical Recommendations	Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.		
24	Technical Recommendations	Ensure that encryption key sizes are at least 128-bits or as large as possible.		
25	Technical Recommendations	Make sure that default shared keys are periodically replaced by more secure unique keys.		

26	Technical Recommendations	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).		
27	Technical Recommendations	Install antivirus software on all wireless clients.		
28	Technical Recommendations	Install personal firewall software on all wireless clients.		
29	Technical Recommendations	Disable file sharing on wireless clients (especially in untrusted environments).		
30	Technical Recommendations	Deploy MAC access control lists.		
31	Technical Recommendations	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.		
32	Technical Recommendations	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.		
33	Technical Recommendations	Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.		
34	Technical Recommendations	Fully test and deploy software patches and upgrades on a regular basis. !		
35	Technical Recommendations	Ensure that all APs have strong administrative passwords. !		
36	Technical Recommendations	Ensure that all passwords are being changed regularly. !		
37	Technical Recommendations	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.		
38	Technical Recommendations	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	Technical Recommendations	Use static IP addressing on the network.		
40	Technical Recommendations	Disable DHCP.		
41	Technical Recommendations	Enable user authentication mechanisms for the management interfaces of the AP.		
42	Technical Recommendations	Ensure that management traffic destined for APs is on a dedicated wired subnet.		
43	Technical Recommendations	Use SNMPv3 and/or SSL/TLS for Web-based management of APs.		
44	Operational Recommendations	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	Operational Recommendations	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.		
46	Operational Recommendations	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.		
47	Operational Recommendations	Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.		
48	Operational Recommendations	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		
49	Operational Recommendations	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.		
50	Operational Recommendations	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		
51	Operational Recommendations	Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.		
52	Operational Recommendations	Fully understand the impacts of deploying any security feature or product prior to deployment.		

53	Operational Recommendations	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.		
54	Operational Recommendations	Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.		
55	Operational Recommendations	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	Operational Recommendations	If the access point supports logging, turn it on and review the logs on a regular basis		