



Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	No: NYS-S15-003
IT Standard: 802.11 Wireless Network Security	Updated: 09/11/2018
	Issued By: NYS Office of Information Technology Services Owner: Chief Information Security Office

1.0 Purpose and Benefits

The purpose of this standard is to establish controls for 802.11 wireless networks in order to minimize risks to the confidentiality, integrity and availability of State Entity's (SE) information and to support secure access to State resources and services over SE wireless networks.

802.11 wireless networks enable users of wireless devices the flexibility to physically move throughout a wireless environment while maintaining connectivity to the network. While 802.11 wireless networks are exposed to many of the same risks as wired networks, they are also exposed to additional risks unique to wireless technologies. This standard outlines the additional controls required for the use of wireless networks by SEs.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117* provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, [NYS-P08-002 Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines.](#)

3.0 Scope

This standard applies to all “State Government” entities as defined in Executive Order 117 or “State Agencies” as defined in Section 101 of the State Technology Law (“State Entities”), their employees, and all others, including third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. Where a conflict exists between this standard and a State Entity’s standard, the more restrictive standard will take precedence.

This standard applies to all 802.11 wireless networks that store, process, or transmit SE data or connect to a SE network or system, including networks managed and hosted by third parties on behalf of the State.

The types of 802.11 wireless networks in scope include:

- Internal – these SE wireless networks are directly connected to the State’s internal information technology resources and are only available to authenticated users.
- Public (authenticated) – these SE wireless networks are not connected to the State’s internal information technology resources and access is limited to authenticated users.
- Public (non-authenticated) – these SE wireless networks are not connected to the State’s internal information technology resources and are available for anyone to use without authentication.

4.0 Information Statement

1. 802.11 wireless networks must follow all requirements of the [NYS Information Security Policy](#) including, but not limited to, a risk assessment prior to implementation.
2. All wireless installations must be authorized by the management of the SE whose data will traverse the wireless network.
3. Security plan documentation, as required by the [Secure System Development Lifecycle Standard](#), must include, at a minimum, the department name, all AP locations, all supporting wireless infrastructure locations, the subnet on the wired network, and the Service Set Identifier (SSID).
4. APs and other supporting wireless devices must be placed in a physically protected location that minimizes opportunity for theft, damage or unauthorized access.

5. Wireless network coverage must be managed to restrict the ability to connect outside of the SE-approved boundary.
6. The SSID of 802.11 wireless networks must be changed from the factory default setting.
7. The SSID must not include information that indicates the location, technology or manufacturer details of the wireless network (e.g., Server-Rm-WiFi-Access, Wifi-Rm70 and Cisco-2400-WiFi). The SSID also must not include information that indicates the type of data traversing the network.
8. A wireless intrusion detection system (IDS) must be utilized on all SE internal wireless networks.
9. Public wireless networks must be, at a minimum, physically separated from the internal network or configured to tunnel to a secure endpoint outside the internal network. The design must be included in the documented security plan.
10. Logical addressing schemas used for the wireless network must differ from those used for the wired network in order to effectively distinguish client connections between the two networks.
11. While servers and information stores may be accessible over a wireless network, they must not directly connect to a wireless network.
12. APs on public authenticated or internal wireless networks must be configured to provide the strongest encryption settings available. At a minimum, Wi-Fi Protected Access (WPA) 2 – Advanced Encryption Standard (AES) must be utilized.
13. WPA2 personal mode must not be used for internal State networks.
14. WPA2 personal mode, with Wi-Fi Protected Access (WPS) disabled, may be used for public authenticated access points that do not connect to internal State networks.
15. APs which utilize passphrases (such as APs configured to use WPA2 personal mode) must use passphrases that conform to the NYS Authentication Tokens Standard and must be at least 12 characters in length and changed at minimum every six months.
16. Passphrases used by APs must be changed from the factory default setting.
17. The wireless network administration console must not be directly accessible from the wireless network.
18. 802.1X authentication, specifically the Extensible Authentication Protocol (EAP), must be used for all devices connecting to the internal State wireless networks. SEs must use the EAP-TLS method whenever possible. Use of Lightweight EAP (LEAP) or use of the following EAP authentication mechanisms is not allowed:

EAP-MD5 (Message Digest), EAP-OTP (One Time Password), and EAP-GTC (Generic Token Card).

19. Wireless client devices that connect to internal wireless networks must be configured to validate certificates issued by the authentication server during the authentication process.
20. Wireless client devices must be configured to utilize identity privacy settings during the authentication process, where technically feasible.
21. Individual user authentication, in accordance with the Authentication Token Standard, is required for SE internal wireless networks.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Chief Information Security Office [exception process](#).

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

Term	Definition
Access Point (AP)	A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired Local Area Network.
Service Set Identifier (SSID)	A 32-character unique identifier. The SSID is the identifier that differentiates one wireless network from another; so all access points and all devices attempting to connect to a specific wireless network must use the same SSID. An SSID is essentially the numeric name of the network.
Wireless Local Area Network (WLAN)	A group of wireless networking nodes within a limited geographic area that serve as an extension to existing wired local area networks, and which are based on the IEEE 802.11 standard and its amendments.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S15-003
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: EISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: <http://www.its.ny.gov/tables/technologypolicyindex>

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
05/15/2015	Original Standard Release	Deborah A. Snyder, Deputy Chief Information Security Officer
02/15/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/11/2018	Scheduled review – minor change to Authority, Scope and title of office	Deborah A. Snyder, Chief Information Security Officer

9.0 Related Documents

[NYS IT Standard-S14-009 - NYS Mobile Device Security Standard](#)

[NYS IT Standard – S14-007 – NYS Encryption Standard](#)

[NIST Special Publication 800-48 Revision 1](#) - Guide to Securing Legacy IEEE 802.11 Wireless Networks

[NIST Special Publication 800-97](#) - Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

[NIST Special Publication 800-153](#) - Guidelines for Securing Wireless Local Area Networks (WLANs)