



Office of Information Technology Services

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

| | |
|---|---|
| <p>New York State Information Technology Standard</p> | <p>No: NYS-S15-003</p> |
| <p>IT Standard:</p> <p>802.11 Wireless Network Security</p> | <p>Updated: 03/11/2025</p> <p>Issued By: NYS Office of Information Technology Services</p> <p>Owner: Chief Information Security Office</p> |

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 (SE) information, and to support secure access to such information and State Information Technology (IT) 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. 117¹*, issued January 2002, 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

¹ All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, [NYS-P08-002 Authority to Establish Enterprise Information Technology Policies, Standards, and Guidelines](#).

3.0 Scope

This standard applies to all “State Entities” (SE), defined as “State Government” in Executive Order 117 or “State Agencies” as defined in Section 101 of the State Technology Law. This includes employees and all other third parties (such as local governments, consultants, vendors, and contractors), that use or access any Information Technology (IT) Resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different standard, it must include the requirements set forth in this one. Where a conflict exists between this standard and an SE’s standard, the more restrictive standard will take precedence.

This standard applies to all 802.11 wireless networks that store, process, or transmit SE information or connect to an 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 IT Resources and are only available to authenticated users.
- Restricted Use – these SE wireless networks are segmented from the State’s internal IT Resources, are only available to authenticated users and SE devices, and are commonly used for Operational Technology (OT) as well as limited Information Technology (IT). Examples may include HVAC/Building Management systems, laboratory equipment, kiosks, etc. This may include Internet Only networks for SE business purposes.
- Public (authenticated) – these SE wireless networks are not connected to the State’s internal IT Resources and access is limited to authenticated users.
- Public (non-authenticated) – these SE wireless networks are not connected to the State’s internal IT Resources and are available for anyone to use without authentication.

4.0 Information Statement

802.11 wireless networks must meet the following minimum requirements:

1. All requirements of the [NYS-P03-002 Information Security Policy](#) including, but not limited to, a risk assessment prior to implementation must be followed
2. All requests must be authorized by the management of the SE whose information will traverse the wireless network.

3. Security plan documentation, as required by the [NYS-S15-003 Secure System Development Life Cycle Standard](#) must include, at a minimum, the SE name, all Access Point (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 physically protected locations that minimize the 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-Room-Wi-Fi-Access," "Wi-Fi- Room70," "Cisco-2400-Wi-Fi"). 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 (authenticated and non-authenticated) must be, at a minimum, physically separated from the internal wireless network or configured to tunnel to a secure endpoint outside the internal wireless network. The design must be included in the documented security plan.
10. Logical addressing schemas must be used for public wireless (authenticated and non-authenticated), internal wireless, and wired networks in order to effectively distinguish client connections between them.
11. While servers and information stores may be accessible over a wireless network, they must not directly connect to any 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 cannot be used for SE internal wireless 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 SE internal wireless networks.
15. 802.1X authentication, specifically the Extensible Authentication Protocol (EAP), must be used for all devices connecting to SE internal wireless networks. SEs must use the EAP-TLS (Transport Layer Security) method whenever possible. Use of Lightweight EAP (LEAP) or any of the following EAP authentication mechanisms is prohibited: EAP-MD5 (Message Digest), EAP-OTP (One Time Password), and EAP-GTC (Generic Token Card).
16. For Restricted Use and Public networks, APs which utilize only passphrases (such as APs configured to use WPA2 personal mode) must use passphrases that

conform to the [NYS-S14-006 Authentication Tokens Standard](#) and must be at least 14 characters in length and changed at a minimum every six months.

- APs which use passphrases in conjunction with other technology, such as iPSK+MAC (individual pre shared key for each authorized MAC address), may be approved to not have regular passphrase changes, subject to/based on a risk assessment of the implementation.
17. Passphrases used by APs must be immediately changed from the factory default setting.
 18. Administrative access to any wireless network devices (APs, routers, etc.) must not be allowed from any wireless network. All administrative access must be performed via the wired network.
 19. Wireless devices that connect to SE internal wireless networks must be configured to validate certificates issued by the authentication server during the authentication process.
 20. Wireless devices must be configured to utilize identity privacy settings during the authentication process, where technically feasible.
 21. Individual user authentication is required for SE internal wireless networks, in accordance with the [NYS-S14-006 Authentication Tokens Standard](#).

5.0 Compliance

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

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 <https://its.ny.gov/glossary>.

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
31 British American Blvd
Latham, NY 12110

Telephone: (518) 242-5200

Email: CISO@its.ny.gov

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

8.0 Revision History

This policy should be reviewed consistent with the requirements set forth in [ITS-P24-003 Process for Establishing Information Technology Policies, Standards and Guidelines.](#)

| 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 |
| 11/23/2021 | Scheduled review – minor changes for clarification and updated Authority and Scope | Karen A. Sorady, Chief Information Security Officer |
| 03/11/2025 | Scheduled review – added additional network type, added language for Access Point (AP) usage, as well as minor language changes | Chris DeSain, Chief Information Security Officer |

9.0 Related Documents

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

[NYS-S14-007 Encryption](#)

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

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