|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **802.11 Wireless Network Security Standard** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 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 information and to support secure access to resources and services over 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.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

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

The types of 802.11 wireless networks in scope include:

* Internal – these wireless networks are directly connected to the internal information technology resources and are only available to authenticated users.
* Public (authenticated) – these wireless networks are not connected to internal information technology resources and access is limited to authenticated users.
* Public (non-authenticated) – these wireless networks are not connected to 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 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 entity 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 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 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 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 networks.
15. APs which utilize passphrases (such as APs configured to use WPA2 personal mode) must use passphrases that conform to the 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 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 internal wireless networks.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended 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, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | Definition |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Revision History

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

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 9.0 Related Documents

Mobile Device Security Standard

Encryption Standard