Queens College	No: QC-ITS-Cyber-003
802.11 Wireless Network Security Standard	**Updated: 08/21/2023**
	Issued By: Queens College, Office of Chief Information Security Officer **Owner: Queens College Information Technology Services**

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

- **Responsible Office(s):** Queens College Information Technology Services
- **Responsible Executive(s)**: Chief Information Officer
- **Responsible Officer(s)**: Chief Information Security Officer

3.0 Scope: College-Wide

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 Policy Statement

1. 802.11 wireless networks must follow all requirements of the Information Security Policy, including, but not limited to, a risk assessment before 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 (ITS), 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 the 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. If available, 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 to distinguish client connections between the two networks effectively.

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. Passphrases used by APs must be changed from the factory default setting.
16. The wireless network administration console must not be directly accessible from the wireless network.
17. Wireless client devices that connect to internal wireless networks must be configured to validate certificates issued by the authentication server during the authentication process.
18. Wireless client devices must be configured to utilize identity privacy settings during the authentication process, where technically feasible.
19. Individual user authentication, in accordance with the Authentication Token Standard, is required for internal wireless networks.

5.0 Compliance

This standard 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 standard is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:
Chief Information Security Officer
Damon Vogel
CISO@qc.cuny.edu

8.0 Revision History

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

Date	Description of Change	Reviewer
10/18/2022	Initial Changes to apply to Queens College	DVogel
6/12/2023	Secondary Changes for QC & Tags Applied	DVogel
08/21/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

QC-ITS-Cyber-020: Mobile Device Security Standard

QC-ITS-Cyber-012: Encryption Standard

10.0 External Documents