NATIONAL DATA
MANAGEMENT AUTHORITY

802.11 Wireless Network Security Standard

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This standard establishes controls for 802.11 wireless networks.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

The purpose of this standard is to establish controls for 802.11 wireless networks in order to minimise 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

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard encompasses all systems and infrastructure, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It specifically addresses 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 Government.

The types of 802.11 wireless networks in scope include:

3.1 Internal – these wireless networks are directly connected to the internal information technology resources and are only available to authenticated users.

3.2 Public (authenticated) – these wireless networks are not connected to internal information technology resources and access is limited to authenticated users.

3.3. Public (non-authenticated) – these wireless networks are not connected to internal information technology resources and are available for anyone to use without authentication.

It is the user's responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

4.1 802.11 wireless networks must follow all requirements of the Information Security Policy including, but not limited to, a risk assessment prior to implementation.

4.2 All wireless installations must be authorised by the management of the organisation whose data will traverse the wireless network.

4.3 Security plan documentation, as required by the Secure System Development Lifecycle Standard, must include, at a minimum, the department name, all Access Point (AP) locations, all supporting wireless infrastructure locations, the subnet on the wired network, Service Set Identifier (SSID), and the wireless authentication protocol used for wireless network users.

4.4 APs and other supporting wireless devices must be placed in a physically protected location that minimises opportunity for theft, damage or unauthorised access.

4.5 Wireless network coverage must be managed to restrict the ability to connect outside of the approved boundary.

4.6 The SSID of 802.11 wireless networks must be changed from the factory default setting.

4.7 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.

4.8 A wireless intrusion detection system (WIDS) must be utilised on all internal wireless networks.

4.9 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.

4.10 Logical addressing schemas used for the wireless network must differ from those used for the wired network to effectively distinguish client connections between the two networks.

4.11 While servers and information stores may be accessible over a wireless network, they must not directly connect to a wireless network.

4.12 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 utilised.

4.13 WPA2 personal mode must not be used for internal networks.

4.14 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.

4.15 APs which utilise 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.

4.16 Passphrases used by APs must be changed from the factory default setting.

4.17 The wireless network administration console must not be directly accessible from the wireless network.

4.18 802.1X authentication, specifically the Extensible Authentication Protocol (EAP), must be used for all devices connecting to the internal wireless networks. Secure Elements (SEs) must use the Extensible Authentication Protocol–Transport Layer Security (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).

4.19 Wireless client devices that connect to internal wireless networks must be configured to validate certificates issued by the authentication server during the authentication process.

4.20 Wireless client devices must be configured to utilize identity privacy settings during the authentication process, where technically feasible.

4.21 Individual user authentication, in accordance with the Authentication Token Standard, is required for internal wireless networks.

4.22 Unused services, ports, and network connections on AP's and authenticated servers must be disabled.

4.23 Monitoring and auditing of wireless networks must be done in compliance with the *Security Logging Standard.*

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the standard may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this standard shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this standard.

8.0 Definitions of Key Terms

Term	Definition
Access Point (AP)[1]	A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.
Service Set Identifier (SSID)[2]	A name assigned to a wireless access point that allows stations to distinguish one wireless access point from another.
Wi-Fi Protected Access 2 (APA-2)[3]	The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For federal government use, the implementation must use federal information processing standards (FIPS) approved encryption, such as advanced encryption standard (AES).
Wireless Intrusion Detection System (WIDS)[4]	A commercial wireless technology that assists designated personnel with the monitoring of specific parts of the radio frequency (RF) spectrum to identify unauthorised wireless transmissions and/or activities.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[1] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/access_point

[2] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/ssid

[3] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/wi_fi_protected_access_2

[4] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/wireless_intrusion_detection_system