Office of the Chief Information Officer Directive: IT 10.04	Published: 04/2019
Chapter: Network Security	Last Review: 01/2022
Subject: **Wireless Network**	

1 DIRECTIVE

1.01 Wireless network connectivity must be implemented using industry-best precautions and setup parameters with respect to security.

1.02 When wireless network connectivity is implemented, Network Planning and IT Support must re-evaluate security risks at least quarterly with respect to known security exposures. This evaluation may result in:

(a) Suspension of wireless support until the risk can be reduced;

(b) Implementation of additional restrictions on wireless connectivity;

(c) Implementation of new hardware and/or software to lessen or eliminate new risks.

1.03 Users employing devices that are enabled for wireless connection to the GNB network must observe all rules for preventing unauthorized access to the network, preventing unauthorized use of the devices themselves, and the mandatory use of passwords and authentication appliances.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that wireless connectivity to the GNB's network does not unduly increase the threat of loss or damage to the GNB's IT resources and data.

3 SCOPE

3.01 This directive applies to Network Planning, IT Support and all users of wireless devices enabled for network connectivity.

4 RESPONSIBILITY

4.01 Network Planning is responsible:

(a) To design wireless network access to minimize security risks

(b) To remain informed about the latest wireless network threats

(c) To plan upgrades to keep GNB networks secure from new threats

4.02 IT Support is responsible:

(a) To configure wireless equipment to eliminate or minimize risks

(b) To remain informed about the latest wireless network threats

(c) To manage wireless risks as required, including suspending wireless service when security threats are discovered

4.03 Users of equipment configured for wireless connectivity are responsible to follow the direction of IT Support to minimize security risks when their wireless devices are enabled for network connectivity.

5 DEFINITIONS

5.01 "**802.11**" is family of specifications for wireless local area networks developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The family includes several specifications, including 802.11a, 802.11b, 802.11g, and 802.11i. Additional specifications are expected to address ongoing changes in performance or security.

5.02 "**AES**" (**Advanced Encryption Standard**) is a 128-bit block data encryption technique developed by Belgian cryptographers John Daemon and Vincent Rijmen that replaced the DES encryption algorithm used by the US government until October 2000.

6 RELATED DIRECTIVE

OCIO IT 9.06 – Data Encryption
OCIO IT 10.01 – Network Hardware Connection
OCIO IT 10.02 – Firewall Protection
OCIO IT 10.03 – Remote Access
OCIO IT 10.08 – Instant Messaging
OCIO IT 13.02 – Data Access & Data Protection
OCIO IT 13.03 – Passwords – Selection & Control
OCIO IT 13.06 – Clear and Locked Screen
OCIO IT 13.07 – Removable Media
OCIO IT 13.08 – Portable Computers
OCIO IT 13.09 – Remote Access – Users