

1 DIRECTIVE

- 1.01 Direct connection of computer equipment to the GNB network is restricted to:
- (a) GNB-owned and supplied computers with a system image as defined and maintained by IT Support.
 - (b) Personally-owned computers (e.g., laptops, tablets, and smart phones) only at defined access points that are external to the secure GNB internal network.
- 1.02 Computers connected directly to the GNB's secure network may not have a wireless network adapter enabled at the same time.

2 PURPOSE

- 2.01 The purpose of this Directive is to ensure that:
- (a) GNB systems are protected against security threats from computer systems managed outside the GNB's control.
 - (b) GNB systems are not exposed to wireless threats from outside the GNB's secure network.

3 SCOPE

- 3.01 This directive applies to all GNB networks and network-connected appliances, servers, and computer systems.

4 RESPONSIBILITY

- 4.01 All employees and guests are responsible to observe the restrictions imposed on computer systems that may be connected to the GNB network.
- 4.02 The Network Architect is responsible to ensure that the network design incorporates industry-best network connection protection at each network access point, system server, and GNB provided computing device.
- 4.03 IT Technical Support is responsible to provide a secure and maintainable system image for all GNB owned or manager computer systems with direct connection capability to the secure GNB network.

Office of the Chief Information Officer Directive: IT 10.01 Chapter: Network Security Subject: Network Hardware Connection	Published: 04/2019 Last Review: 01/2024
--	--

5 DEFINITIONS

- 5.01 **“Access point”** is a hardware device that acts as a communication hub for a network and permits computer devices to connect to the network. Connection is accomplished either through a cable connecting the hub directly to the computer or through a wireless interface that establishes a connection with a wireless-capable computer.

6 RELATED DIRECTIVES

- OCIO IT 10.02 – Firewall Protection
- OCIO IT 10.03 – Remote Access
- OCIO IT 10.04 – Wireless Network
- OCIO IT 10.05 – Network Intrusion Detection
- OCIO IT Chapter 13 – User Responsibilities