Office of the Chief Information Officer Directive: IT 13.09	Published: 04/2019
Chapter: User Responsibilities	Last Review: 01/2022
Subject: **Remote Access – Users**	

1 DIRECTIVE

1.01 Users who need remote access must have management approval to connect to the company's IT facilities from an offsite location.

1.02 Users with the capability to connect remotely to GNB Information Security Directive's IT facilities:

(a) Must follow the security guidance supplied by IT Technical Support regarding who has access to their computing devices, configuration of their remote connection software, and maintenance of their operating system.

(b) Must not use non-company email accounts, such as Hotmail, Yahoo or AOL to conduct company business.

(c) Must observe the same restrictions regarding the use of company facilities and resources while connected remotely as are defined in all User Responsibilities policies for onsite use.

(d) Must not disable or circumvent any company-imposed security measures such as antivirus software or idle activity limits and associated automated action.

(e) Must maintain their remote systems with all available security patches in a timely manner.

(f) Must maintain up-to-date antivirus definitions and software.

(g) May only enable wireless connection capability on a network-connected client computer or laptop with the written consent of IT Technical Support.

(h) Must not divulge to an unauthorized individual the remote configuration parameters that enable their remote connection to GNB Information Security Directive**'s** IT facilities.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that:

(a) Users with approved remote access capability have secure means to access GNB Information Security Directive's information systems.

(b) Company systems, networks, and data are adequately protected against security threats from computer systems managed outside GNB Information Security Directive's premises and control.

(c) Only authorized users with appropriate training regarding safe remote access procedures may connect to company systems and networks via remote connections.

3 SCOPE

3.01 This Directive applies to all users granted remote access to company IT resources.

4 RESPONSIBILITY

4.01 **IT Technical Support** is responsible to provide remote connection users with information that helps them understand the importance of and common methods for securing their home networks and portable computers.

4.02 Remote access users are responsible to:

(a) Have documented management approval with business justification to connect from an offsite location.

(b) Limit their remote access to those computing devices and networks that are approved by IT Technical Support.

(c) Limit remote access on their computing devices to users approved by management (no family, friends, visitors or intruders).

(d) Configure and maintain computing devices which access company IT resources from a remote location per the Directive statement above.

(e) Protect their remote access mechanisms (identity, passwords, appliances, etc.) against unauthorized use or loss.

(f) Keep personal equipment with remote access capability in secure environments.

(g) Refrain from being connected to GNB Information Security Directive's site and simultaneously connected to any other network with the exception of a personal network that is under the complete control of the user.

(h) Refrain from bypassing any security mechanisms required by IT Technical Support such as idle activity timeouts and action on either the user's system or at GNB Information Security Directive's site (e.g., 30 minutes without keyboard or mouse activity, automatic reconnect and logon, ping to simulate non-idle network connection).

5 DEFINITIONS

5.01 "**VPN**" (**Virtual Private Network**) is the configuration of a secure encrypted communication channel or tunnel through a public network such as the Internet.

6 RELATED DIRECTIVES

OCIO IT 10.03 – Remote Access

OCIO IT 10.04 – Wireless Network

OCIO IT 10.08 – Instant Messaging

OCIO IT 13.01 – System Access and Acceptable Use

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 14.01 – BYOD: Acceptable Devices and Operating Systems
OCIO IT 14.02 – BYOD: System Access and Acceptable Use