Office of the Chief Information Officer Directive: IT 10.03	Published: 04/2019
Chapter: Network Security	Last Review: 01/2022
Subject: **Remote Access**	

1 DIRECTIVE

1.01 Remote access mechanisms may be implemented to access GNB internal systems, networks and data only if:

(a) Remote access can be justified to achieve a business or operational goal;

(b) Remote access can be implemented with sufficient security to minimize the risks of exposing GNB systems, networks and data.

1.02 Each remote access mechanism must be cost-justified and risk-justified on its own merits.

1.03 Remote access may be granted only to those users who have a business need to connect from an offsite location. All users must be approved by their managers.

1.04 A user accessing a GNB system using a remote connection must:

(a) Ensure that equipment used to connect to GNB networks meets GNB requirements for remote access;

(b) Not be simultaneously connected to any other network with the exception of a personal network that is under the complete control of the user;

(c) Not use non-GNB email accounts, such as Hotmail, Yahoo, AOL, to conduct GNB business.

1.05 Wireless connection capability may only be enabled on a network-connected client computer or laptop with the express consent of IT Support.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that GNB systems, networks and data are adequately protected against external threats that may materialize through the implementation of a remote access mechanism.

3 SCOPE

3.01 This directive applies to:

(a) All GNB systems which are candidates for remote access;

(b) All users authorized to use remote access to GNB systems.

4 RESPONSIBILITY

4.01 The Network Architect is responsible to ensure that, for each remote access mechanism to be implemented:

(a) The business case is cost-justified

(b) The mechanism is configured to minimize risk to an acceptable level and incorporates industry-best controls

(c) Criteria are established for a user to be approved for remote access through the remote access mechanism

4.02 IT Support is responsible to ensure that:

(a) Each remote access mechanism is configured as designed

(b) Every user enabled for each remote access mechanism is authorized

(c) Remote access approvals are reviewed annually for all authorized users

(d) Remote access resources are used only for GNB business when needed

(e) Wireless connectivity is detectable in a security-sensitive IT installation

4.03 Remote access users are responsible to:

(a) Protect their remote access mechanisms (passwords, appliances, etc.) against unauthorized use;

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

5 DEFINITIONS

5.01 "**SSL**" (**Secure Sockets Layer**) 3.0 is the current widely deployed protocol used for providing a secure communications layer for HTTP.

5.02 "**TLS**" (**Transport Layer Security**) is the IETF standards-track protocol for secure TCP/IP communications based on SSL 3.0, but implementing an open and standards-based solution.

5.03 "**IETF**" (**Internet Engineering Task Force**), the main standards organization for the Internet, is an open international community of network designers, operators, vendors, and researchers concerned with the evolution and smooth operation of the Internet.

5.04 "**SSL/TLS**" is a negotiated level of communications security, a secure communications layer on top of TCP/IP.

5.05 "**HTTPS**" is the communications security protocol for TCP/IP established by using HTTP over SSL/TLS.

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

6 RELATED DIRECTIVES

OCIO IT 9.06 – Data Encryption
OCIO IT 10.01 – Network Hardware Connection
OCIO IT 10.02 – Firewall Protection
OCIO IT 10.04 – Wireless Network
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