Office of the Chief Information Officer Directive: IT 13.01	Published: 04/2019
Chapter: User Responsibilities	Last Review: 01/2022
Subject: **System Access and Acceptable Use**	

1 DIRECTIVE

1.01 All users must restrict their use of GNB IT systems to those activities deemed acceptable by management, which are those broadly defined as business use to further the interests of the GNB.

1.02 All data entered and maintained on GNB IT systems is owned by GNB. Users must not have any expectation of privacy regarding data entered or maintained on GNB equipment. GNB administrators may access or examine all user files or accounts that are suspected of unauthorized use or misuse. Misuse may be prosecuted under applicable civil law or reported to the justice system for prosecution under applicable criminal law.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that the GNB is protected against:

(a) Security threats to IT systems from authorized IT systems users;

(b) Response and scheduling issues on IT systems from excess unplanned system usage;

(c) Abuse of GNB assets;

(d) Civil or criminal liability arising from illegal activities perpetrated on GNB systems;

(e) Civil liability arising from unauthorized violations of terms of applicable software licensing agreements and copyright laws.

3 SCOPE

3.01 This directive applies to all users authorized to use GNB IT systems.

4 RESPONSIBILITY

4.01 All authorized IT systems users are responsible to limit their use of the system to authorized GNB business pursuits.

4.02 IT Operations is responsible, under the supervision of GNB management, to access or examine user files or accounts that are identified as suspected of unauthorized use or misuse.

4.03 Executive management is responsible to initiate any action arising from the discovery of misuse of GNB IT resources.

5 DEFINITIONS

5.01 "**Acceptable use**" of GNB IT systems is any management-authorized activity that furthers the GNB's business interests. In some cases, department managers may authorize limited personal use of GNB systems for purposes

that:

(a) Are not illegal or immoral, and would not cause embarrassment to the GNB if discovered;

(b) Do not impact any business processes;

(c) Do not use resources so as to require IT resource capacity growth.

6 RELATED DIRECTIVES

OCIO IT 3.05 – Licenses
OCIO IT 3.06 – Software Downloading
OCIO IT 4.04 – Downloading
OCIO IT 6.06 – Performance and Capacity Management
OCIO IT 8.02 – Systems Security
OCIO IT 8.03 – User Identification and Passwords
OCIO IT 8.04 – Confidentiality and Privacy
OCIO IT 8.05 – Controls for Viruses, Worms and Malware
OCIO IT 10.03 – Remote Access
OCIO IT 10.04 – Wireless Network
OCIO IT 10.06 – File Transfer Protocol (FTP)
OCIO IT 10.07 – Email Security
OCIO IT 10.08 – Instant Messaging
OCIO IT 11.11 – End-User Restrictions (during disaster recovery)
OCIO IT 13.02 – Data Access and Data Protection
OCIO IT 13.03 – Passwords