Office of the Chief Information Officer Directive: IT 14.01	Published: 12/2020
Chapter: Mobile Device Management	Last Review: 01/2024
Subject: Acceptable Devices, Use, and Management	

1 DIRECTIVE

1.01 Whenever corporately owned or managed mobile devices are used for business purposes technical and administrative controls will be enforced to protect GNB data.

1.02 Mobile devices with access to GNB enterprise networks or containing GNB data must be configured with GNB controls which may include, but are not limited to:

(a) an approved method of authentication (password, PIN, biometric control, etc.) to enable the device's use

(b) a screen timeout after a GNB acceptable period of inactivity with authentication re-activation

(c) encryption that is enabled for GNB data in transit and at rest by default

(d) a GNB-approved malware protection (antivirus, firewall, spyware, etc.) is installed on mobile devices

(e) a GNB approved mobile device management service that includes:

i. remote data-wipe capability

ii. mobile device hardening to minimize security vulnerabilities

2 PURPOSE

2.01 To ensure that GNB can securely manage and support its mobile devices and protect the GNB data they transmit or store.

3 SCOPE

3.01 Applies to corporately owned or managed mobile devices that handle GNB data.

4 RESPONSIBILITY

4.01 IT Service Provider is responsible to:

(a) develop and maintain the GNB list of approved mobile devices and platforms

(b) implement and maintain controls on mobile devices that handle GNB data

4.02 Employees are responsible for:

(a) using an approved authentication method (password, PIN, biometric control, etc.) to access the device

(b) promptly reporting security incidents and lost or stolen devices to the IT Service Provider

(c) personal applications and data.

4.03 GNB executive management is responsible to authorize any action arising from the discovery of breaches of mobile device policies or directives.

5 DEFINITIONS

5.01 Mobile Device – any externally connected device that handles GNB data.

6 RELATED DIRECTIVES

OCIO IT 9.02 – Data Classification
OCIO IT 9.03 – Data Access Controls
OCIO IT 13.01 – System Access and Acceptable Use
OCIO IT 13.03 – Passwords
OCIO IT 13.04 – Email Acceptable Use
OCIO IT 13.05 – Internet Access and Acceptable Use
OCIO IT 13.07 – Removable Media
OCIO IT 14.05 –Acceptable Devices, Use, and Management