

1 DIRECTIVE

- 1.01 All users enrolled in the company’s BYOD program must sign an agreement that the company has the authority to:
- a. restrict which personal applications may be installed on the user’s BYOD device.
 - b. restrict the copying of corporate data residing on the device to an external device or backup service.
 - c. inspect their BYOD device on demand to review personally-owned applications installed on the device.
 - d. wipe the device remotely* if it is lost or stolen, or the user leaves the organization.

*Note: this includes personal data such as email, contacts, calendar appointments, personal pictures, music, games, network connections, etc.

2 PURPOSE

- 2.01 The purpose of this Directive is to ensure that corporate data and enterprise networks are protected against:
- a. known rogue applications inadvertently installed on a BYOD device by an unsuspecting employee.
 - b. exposure on an unprotected storage device or an external storage provider.
 - c. access by an unauthorized user of an approved BYOD device that has been misplaced or lost.

3 SCOPE

- 3.01 This Directive applies to all users, permanent, temporary or contract, when they are authorized to access company IT systems using their own computing devices.

4 RESPONSIBILITY

- 4.01 All prospective BYOD users are responsible to sign an agreement that their approved devices are subject to controls identified by the company and to inspection on demand.
- 4.02 There is currently no compensation by GNB for BYOD users.

5 DEFINITIONS

- 5.01 Mobile Device – any externally connected device that handles GNB data.
- 5.02 “BYOD” – Bring-your-own-device refers to the use of mobile devices owned by

Cyber Security Directive: IT 14.05 Chapter: Mobile Device Management Subject: User Agreements for BYOD Participation	Published: 12/2020 Last Review: 01/2024
---	--

entities other than GNB.

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 14.01 –Acceptable Devices, Use, and Management