Office of the Chief Information Officer Directive: IT 5.02	Published: 02/2020
Chapter: Data Management	Last Review: 01/2022
Subject: **Data Backup and Storage**	

1 DIRECTIVE

1.01 Data must be backed up and stored in a protected location on a regular basis.

1.02 For data critical to the ongoing operation of the business, a copy of the current backup data must be made at the end of each backup process and transferred to a designated offsite storage location.

2 PURPOSE

2.01 The purpose of this Directive is to specify the procedures to backup data and to allow for recovery of important data in the event of accidental or intentional corruption, loss or destruction of the data.

2.02 For data critical to the ongoing operation of the business, backup data kept at an offsite storage location will facilitate keeping the business operational in the event of a physical disaster at the original site.

3 SCOPE

3.01 This directive applies to:

- All employees who create data on their GNB provided computing devices
- All data owners whose data is maintained on a central shared system

4 RESPONSIBILITY

4.01 All departments are responsible to identify ownership for their data that requires backup. For all data that qualifies, the owning department must ensure that procedures are in place to backup their data whenever it is updated and to store the backup copies as required.

5 DEFINITIONS

5.01 "**Critical data**" is that data which is needed to continue the operation of a business.

5.02 "**Data backup**" means making a copy of data such that the copy may be used easily to recreate the original data organized in its original format.

5.03 "**Data medium**" means a physical object on which data may be stored (e.g., magnetic tape, tape cartridge, optical disk (CD-ROM, DVD), and removable hard drive).

5.04 "**Offsite**" means a physical location other than where data is being processed. Its location must be far enough removed so that data stored offsite is not subject to the same physical risk from foreseen disasters. Note that if the objective is to protect against data loss in the event of a building fire or other disaster that restricts access to the building, a location in the same or adjacent building is not suitable as an offsite storage location.

6 RELATED DIRECTIVES

OCIO IT 5.03 – Management of Third-Party Services

OCIO IT 5.07 – Anti-Spam Requirements

OCIO IT 8.04 – Confidentiality and Privacy

OCIO IT 11.04 – Backup Schedule

OCIO IT 11.05 – Backup Files Stored Onsite

OCIO IT 11.06 – Backup Files Stored Offsite