| | |
|---|---|
| **Office of the Chief Information Officer Directive: IT 13.02** | Published: 04/2019 |
| Chapter: User Responsibilities | Last Review: 01/2022 |
| Subject: **Data Access and Data Protection** | |

## 1 DIRECTIVE

1.01 Users may access data to which they are authorized, but must do so using GNB-authorized applications, programs, interfaces and procedures.

## 2 PURPOSE

2.01 The purpose of this Directive is to minimize the risk of data corruption or loss due to improper data creation, access, update or handling.

## 3 SCOPE

3.01 This directive applies to all users authorized to access GNB IT systems and access GNB data.

## 4 RESPONSIBILITY

4.01 All users are responsible to restrict their access to data using GNB-authorized applications, programs, interfaces and procedures.

4.02 IT Technical Support is responsible:

(a) To document the appropriate applications, programs and interfaces for accessing data, and to provide documented procedures for appropriate classification, management and storage of data.

(b) To provide an active data-update control mechanism or procedural controls for shared data or documents eligible to be taken offline for update by a single user at a time and returned to the shared location after update.

4.03 IT System Administrators are responsible to manage users’ authorized access to data corresponding to the data classification and data owner approvals. (See also **CSD IT 9.03 – Data Access Controls**.)

## 5 DEFINITIONS

5.01 “**Check-out**” is a request by a user to a data control mechanism to restrict data from being modified by any other user. If the check-out request is successful, the requesting user may update the data in place or copy it, modify the copy, and replace the original with the updated copy. A strong data control may prevent data from being modified by anybody until it is checked out, and then the user that checked it out is the only party that may modify it. A procedural data control may allow a user to identify data that is currently checked out for updating, but it is up to other users to check on the data’s current status and to avoid updating data that is identified as checked out.

5.02 “**Check-in**” is a request by the user who completed a successful check-out to the data control mechanism to remove the restrictions imposed by the check-out. The check-in request would be made by the user in control after completing the necessary updates and replacing the data.

## 6 RELATED DIRECTIVES

OCIO IT 5.02 – Data Backup and Storage
OCIO IT 9.01 – Data Ownership
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 14.01 – BYOD: Acceptable Devices and Operating Systems
OCIO IT 14.02 – BYOD: System Access and Acceptable Use