Office of the Chief Information Officer Directive: IT 8.03	Published: 04/2019
Chapter: Physical and Systems Security	Last Review: 01/2022
Subject: **User Identification and Passwords**	

1 DIRECTIVE

1.1 Access to a host computer system, network server, or networked GNB provided computing device must be approved by the user's manager who must forward a request for access (through their individual designated on the chart of authorities) to the IT Service Desk.

The organization will control access to information systems and data, including any host computer, network server, networked personal computer and mobile device by implementing robust user authentication and password management policies and procedures for on prem or cloud services.

2 PURPOSE

2.1 The purpose of this Directive is to ensure that:

- There is management approval on file for the specific system access granted to every individual
- Only personnel authorized to access the computer system, network, or servers are granted access
- All activity on the system, network, or servers may be traced to an individual
- User authentication passwords are kept securely
- An individual may be held accountable for all activity logged against his or her user identifier

3 SCOPE

3.1 This directive applies to all employees having system access.

4 RESPONSIBILITY

4.1 Each manager is responsible to assess his employees' job-related system access requirements and approve those employees who have a business need for access.

4.2 **IT Operations** is responsible to:

(a) Maintain user identifier information and keep signed system access requests on file.

(b) Supply users with identifiers and an expired password for first-time access.

(c) Change the user's password to a new expired password on the user's request to assist with suspected password compromise and forgotten passwords.

(d) Create and maintain a system for administering user identification and passwords.

(e) Understand the risks associated with user identifications and passwords.

(f) Design and implement robust password policies based on current best practices.

(g) Reduce the reliance on passwords where possible.

(h) Reduce the burden on users to mitigate password overload.

(i) Implement technological or automated solutions in user identification and password management systems where possible.

(j) Help users to generate strong passwords.

(k) Support and train users.

4.3 The user is responsible to:

(a) Keep his or her password confidential. No sharing of passwords is allowed.

(b) Change his or her password at first use and on a periodic basis consistent with the data classification of the data to which he or she has access.

(c) Follow password creation guidelines for keeping his or her password confidential.

(d) Notify the **IT service desk** of any suspected password disclosure and suspected user identifier misuse.

Note: The user is also responsible for any processing activity attributed to the user identifier.

5 DEFINITIONS

5.1 **"User identifier"** refers to a set of characters uniquely identifying an individual for system access.

6 RELATED DIRECTIVES

OCIO IT 6.02 – Access Administration

OCIO IT 7.02 – Logging Controls

OCIO IT 8.02 – Systems Security

OCIO IT 9.06 – Data Encryption

OCIO IT 13.01 – System Access and Acceptable Use

OCIO IT 13.02 – Data Access and Data Protection

OCIO IT 13.03 – Passwords