Office of the Chief Information Officer Directive: IT 13.06	Published: 04/2019
Chapter: User Responsibilities	Last Review: 01/2022
Subject: **Clear and Locked Screen**	

1 DIRECTIVE

1.01 Users must lock computer screens when devices are unattended.

1.02 Users who view sensitive data should also secure computer screens from unauthorized viewing when their devices are in use. This includes ensuring that screens are cleared or left blank when not actively in use and positioning screens so they are not visible to passers-by and onlookers.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that unauthorized users:

- Cannot access or view confidential data displayed on computer screens; and
- Cannot access confidential data housed in computer systems but not immediately visible on computer screens.

3 SCOPE

3.01 This directive applies to all users authorized to login to the GNB network, whether remotely or on-site.

4 RESPONSIBILITY

4.01 **Chief Information Security Officer (CISO)** is responsible for developing, implementing and maintaining a written, clear and locked screen directive, as well as a complementary clear desk directive.

4.02 **All users** are responsible for properly observing clear and locked screen procedures in the appropriate circumstances.

4.03 **Managers/Supervisors/Team Leads** are responsible for:

a) Modelling the behaviours required by this directive, to act as examples for their teams.

b) Enforcing this directive, by noting and addressing non-compliance, and escalating responses to repeat instances of non-compliance.

c) Evaluating the risk that computer screens may be visible to unauthorized individuals, when planning and choosing the layout of offices and other workstations.

4.04 **IT Technical Support** is responsible for:

(a) Providing tools, equipment and documented processes or procedures to

enable users to easily clear their screens and lock their workstations without having to log off.

(b) Implementing automatic timeout or screen lock, triggered when a workstation has no keyboard, mouse or other detectable user activity for the pre-determined time period.

5 DEFINITIONS

5.01 "**Privacy Screen or Filter**" refers to a plastic screen, placed over the screens of computers or other portable devices so that only someone looking directly at the screen (you) can see the information on the screen. **Shoulder surfers** cannot view the information from either side of the authorized user because the filtered screen appears too dark for information to be readable.

5.02 "**Shoulder surfer**" refers to someone looking over a user's shoulders – literally or figuratively – that is, using direct observation to access information. Shoulder surfers can use their naked eyes or cameras to record users entering passwords or viewing information.

6 RELATED DIRECTIVES

OCIO IT 8.02 – Systems Security
OCIO IT 8.03 – User Identification and Passwords
OCIO IT 8.04 – Confidentiality and Privacy
OCIO IT 9.02 – Data Classification
OCIO IT 9.03 – Data Access Controls
OCIO IT 9.04 – Application Security Controls
OCIO IT 13.10 – Clear Desk Directive
OCIO IT 13.01 – System Access and Acceptable Use
OCIO IT 13.03 – Passwords
OCIO IT 14.02 – BYOD: System Access and Acceptable Use