Office of the Chief Information Officer Directive: IT 13.10	Published: 04/2019
Chapter: User Responsibilities	Last Review: 01/2022
Subject: **Clean Desk**	

1 DIRECTIVE

1.1 All employees must secure documents and devices, or other items containing or providing access to confidential information, by clearing them from desks and other workspaces, or locking them away at the end of the day or when workspaces are otherwise unattended. Otherwise, these items are vulnerable to theft or other misappropriation by unauthorized persons.

2 PURPOSE

2.1 The purpose of this Directive is to ensure that:

- Unauthorized individuals cannot access or view confidential information because of documents or items left unattended on desks or in other workspaces.
- Workspaces convey a professional and otherwise positive corporate image.
- Employees and the organization can experience productivity gains and cost savings generated by clean, organized and uncluttered workspaces.

3 SCOPE

3.1 This Directive applies to all employees.

4 RESPONSIBILITY

4.1 **All employees** are responsible for clearing their desks and otherwise securing confidential information when workspaces are unattended. This includes time when workspaces are unattended for any significant periods during the day, for example during breaks or meetings (or even a short trip to the bathroom).

4.2 **All employees** are responsible for securing any confidential information or items found unattended by others; reminding colleagues to comply with the Directive and assessing whether to report non-compliance (especially where persistent), to their Manager.

4.3 **Managers and Senior Executives** are responsible for modelling the behaviours required by this Directive, by ensuring that they always secure confidential documents and items.

4.4 **Managers/Supervisors/Team Leads** are responsible for enforcing this Directive, by noting and addressing non-compliance, and escalating their responses for repeated instances of non-compliance.

4.5 **Managers/Supervisors/Team Leads** are responsible for reinforcing adherence to this Directive by designing or implementing appropriate reward systems for exceptional compliance with this Directive.

4.6 **IT Technical Support** is responsible for providing tools/equipment and documented processes or procedures to enable employees to clean their desks and otherwise secure confidential information.

4.7 **Managers/Supervisors/Team Leads** responsible for providing supports to enable employees to adhere to this Directive.

4.8 Failure to comply with this Directive can lead to discipline, up to and including dismissal.

5 DEFINITIONS

5.1 "**Shoulder surfing or visual hacking**" occurs when employees access or display sensitive information in a manner which is then seen, read, stolen or otherwise accessed by a curious individual or a malicious hacker.

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 13.01 – System Access and Acceptable Use
OCIO IT 13.03 – Passwords
OCIO IT 13.06 – Clear and Locked Screen
OCIO IT 14.02 – BYOD: System Access and Acceptable Use