| **Office of the Chief Information Officer Directive: IT 8.02** | Published: 04/2019 |
|---|---|
| Chapter: Physical and Systems Security | Last Review: 01/2022 |
| Subject: **Systems Security** | |

## 1 DIRECTIVE

1.01 For server and host computer systems **IT Operations** will control and administer:

- User identification and authentication controls
- User connection access
- User run or execute authority for applications

1.02 Only **IT Support** may install or update any system software, application software, or hardware.

1.03 For computing systems that are connected to a network:

- **IT Support** must approve all hardware as well as system and application software to be installed or upgraded
- User identification and authentication controls to the personal computer must be implemented without “guest“ users allowed

1.04 For an IT installation where the business demands critical production schedules (e.g., service bureaus, outsourced production) **IT Support** must control all hardware and software installs and upgrades on personal systems.

## 2 PURPOSE

The purpose of this Directive is to ensure that:

- All users operating a networked computing system or connected to an enterprise server or host system can be identified and are authorized to do work on these systems
- Only authorized, security-vetted, and fully licensed application and system software is installed on enterprise IT systems

## 3 SCOPE

3.01 This directive applies to all employees and third party providers with responsibilities in **IT Operations** and **IT Support**.

## 4 RESPONSIBILITY

4.01 Managers are responsible to inform **IT Operations** regarding their employee status and employee responsibilities that require specific system authority.

4.02 **IT Operations** is responsible to control user identifiers and authority levels

associated with each user.

4.03 **IT Support** is responsible:

(a) To plan, test, and investigate all system hardware and system and standard application software for security controls and exposures.

(b) To ensure that all system and application software installed on personal and network systems is authorized and licensed.

4.04 **IT Support** is responsible to plan, test, and investigate all custom application software and extensions for system security controls and exposures.

## 5 DEFINITIONS

5.01 **"Administration authority"** refers to special authority to perform tasks that are usually restricted to those individuals who are permitted to change system-related software and environment options.

5.02 **"Guest user"** is a user identification that permits any individual to use a computer system without otherwise proper identification. This identifier is typically authorized to perform very restricted basic activity on a personal computer with no network or host access.

## 6 RELATED DIRECTIVES

OCIO IT 3.01 – Standard Applications

OCIO IT 3.03 – Non-standard Software

OCIO IT 9.03 – Data Access Controls

OCIO IT 13.01 – System Access and Acceptable Use