Office of the Chief Information Officer Directive: IT 4.02	Published: 02/2020
Chapter: Systems Management	Last Review: 02/2024
Subject: **Role-Based User Management**	

1 DIRECTIVE

1.01 For system access control:

(a) All IT users will be assigned a standard set of system privileges based on a template defined by the Information Technology Service Delivery Organization (IT SDO).

(b) Any additional privileges needed by a user must be requested by the user's manager and approved by the Business Owner

1.02 For application and data control:

(a) Any IT process that results in payments or in goods being transferred must involve two or more users for initiation of the process and validation or approval before the process may be completed.

(b) Access to an application or to data that requires specific authorizations must be approved by the application or data owner.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that there are additional controls in place, specifically:

- To detect errors by using multi-step processes, to limit opportunities for employee fraud or theft, and to increase the probability of detection when fraud or misappropriation of assets is attempted.
- To safeguard company computers and networks against inadvertent exposure to external threats.

3 SCOPE

3.01 This directive applies to:

(a) All application and process designers.

(b) All managers who assign process responsibilities.

(c) All system operators with privileges extending beyond a restricted user.

4 RESPONSIBILITY

4.01 The IT SDO in conjunction with the Business Owner is responsible to assess any user's request for additional privileges beyond the basic defined template.

4.02 The IT SDO and Business Owner is responsible to:

(a) Include multi-user involvement during the execution of any process that results in a funds or goods transfer.

(b) Ensure that applications do not need special privileges to be active during execution unless the task at hand needs these privileges.

4.03 Each department manager is responsible to ensure that:

(a) No employee in the department has all the privileges required to execute a controlled process to completion.

(b) All special privileges are removed when an employee changes responsibility within the department or if the employee is transferred out of the department.

4.04 All users who need additional privileges for specific tasks are responsible to ensure that these privileges are active only during the execution of those specific tasks.

5 DEFINITIONS

5.01 **“Separation of duties”** is a security principle that ensures that an individual must not be able to breach security alone.

5.02 **“Least privilege”** is a security principle that ensures that a user should have only those privileges required for the task at hand and no more.

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 9.03 – Data Access Controls
OCIO IT 9.04 – Application Security Controls
OCIO IT 13.01 – System Access and Acceptable Use
OCIO IT 13.09 – Remote Access - Users