Office of the Chief Information Officer Directive: IT 6.02	Published: 02/2020
Chapter: Computing Operations and Support	Last Review: 01/2022
Subject: **Access Administration**	

1 DIRECTIVE

1.01 Access controls for systems, subsystems and other system objects must be implemented and administered on a timely basis. Subsystems and other system objects include databases, networks, applications, and email servers. (See *Definitions*, below, for a definition and list of system objects.)

2 PURPOSE

2.01 The purpose of this Directive is to ensure appropriate, timely, consistent and efficient administration of access control points.

3 SCOPE

3.01 This directive applies to:

- All owners of systems and other access control points such as applications, databases, networks, email servers and websites
- All computing operations personnel and other staff to whom administration of access control points has been delegated

4 RESPONSIBILITY

4.01 Access control point owners are responsible

(a) To define access privilege criteria.

(b) To review and approve access requests.

(c) To review access privileges at least annually.

4.02 Administrators of access control points are responsible

(a) To maintain contact information for users granted access to any control point.

(b) To change access privileges in a timely manner based on documented management and control point owner requests.

(c)

5 DEFINITIONS

5.01 "**Access control point**" is the computer or appliance that approves the connection to the network. The connection is approved based on identification and authentication for both the computer and the user attempting to complete the connection. Identification of the computer may be simplified in a closed wired network by having the computer supply only a computer name without any authentication. For a wireless connection, computers can supply the MAC

address for its wireless adapter by establishing communication with a wireless access point. The user's identification is completed by supplying a user identifier and authenticating it with a password or an appliance connected to the computer.

5.02 "**MAC address**" is short for Media Access Control address. It is a unique identification code assigned to network hardware such as Network Interface Cards (NIC) including Wireless Fidelity (WiFi) adapters. The MAC address is hard-wired on each device when it is manufactured. Address assignment is controlled in address blocks for each hardware manufacturer by the Institute for Electrical and Electronics Engineers (IEEE) Standards Association to guarantee uniqueness.

5.03 "**System objects**" referred to in this policy are those parts of a system to which access may be controlled on an individual and varying basis. System access does not provide implicit access to any controlled system objects. System objects include, but are not limited to, databases, networks, applications, the Internet, email servers, FTP servers, tape libraries, and company websites.

6 RELATED DIRECTIVES

OCIO IT 4.03 – Internet Access
OCIO IT 5.04 – Database Management
OCIO IT 7.02 – Logging Controls
OCIO IT 8.02 – Systems Security
OCIO IT 8.03 – User Identification and Passwords
OCIO IT 9.03 – Data Access Controls