Office of the Chief Information Officer Directive: IT 13.03	Published: 04/2019
Chapter: User Responsibilities	Last Review: 01/2024
Subject: **Passwords**	

1 DIRECTIVE

1.01 The organization will control access to information systems and data, including any host computer, network server, networked personal computer and mobile device, by implementing robust user authentication and password management policies and procedures.

2 PURPOSE

2.01 The purpose of this Statement of Policy and Procedure is to ensure that, among other things:

- Only personnel authorized to access the computer system, network or servers are granted access
- All activity on the system, network or servers may be traced to a unique individual
- User authentication passwords are strong and kept securely
- An individual may be held accountable for all activity logged against his or her user identifier

3 SCOPE

3.01 This directive applies to all employees.

4 RESPONSIBILITY

4.01 The IT administrator is responsible for:

- Creating and maintaining a system for administering user identification and passwords, which reduce the burden or password overload which users face.
- Helping users to generate strong passwords.
- Otherwise supporting and training users.

4.02 Each department manager or head is responsible for assessing and approving their employees' or other users' (e.g., third-party contractors) business-related system access requirements. This will be based on principles of least-access, or least-privilege necessary.

4.03 All IT systems users are responsible for following this policy as well as **OCIO IT 8.03 – User Identification and Passwords**.

5 DEFINITIONS

5.01 "**Password**" refers to a secret alphanumeric value used to authenticate a user to an information technology resource.

6 RELATED DIRECTIVES

OCIO IT 6.02 – Access Administration
OCIO IT 8.03 – User Identification and Passwords
OCIO IT 10.03 – Remote Access
OCIO IT 13.01 – System Access and Acceptable Use
OCIO IT 13.02 – Data Access and Data Protection
OCIO IT 14.01 – BYOD: Acceptable Devices and Operating Systems
OCIO IT 14.02 – BYOD: System Access and Acceptable Use
OCIO IT 14.03 – Security for BYOD Devices