# IT Policy 7.01

# (Information Technology)

---

**Subject:** **PASSWORD POLICY**

**Scope:** **ALL COUNTY, LIBRARY, LODGE AND CONTRACT EMPLOYEES**

**Issued:** **September 8, 2015**

**Revised:** **February 14, 2023**

## Purpose

The Password Policy defines the use of secure passwords, passphrases, or personal identification numbers to secure sensitive data or information on servers, systems, devices, websites, or software used by staff at Middlesex County.

## Definitions

**"Biometric Security"** is the use of a uniquely identifiable human characteristic for securing sensitive data or information. This includes (but is not limited to) fingerprint, voice, or facial recognition.

**"Core Infrastructure"** is any device connected to the Middlesex County Network which is responsible for providing a critical service or function, such as a firewall, switch, or server.

**"ITS"** means Information Technology Services.

**"Middlesex County ITS"** is the department at Middlesex County responsible for procurement, maintenance, and support of Information Systems.

**"Password"** is a word or a string of characters which allows access to a computer system or service.

**"Passphrase"** is a string of words, traditionally longer than a password, which allows access to a computer system or service.

**"Personal identification Number (PIN)"** is a numerical code which is used to unlock or grant access to a computer system or service.

**"Privileged Access Management (System)"** is a solution designed to securely store, monitor, and audit privileged credential usage for any device considered to be Core Infrastructure.

## Policy

Passwords, passphrases, and personal identification numbers (PINs) shall be used to restrict access to workstations, systems, servers, or services.

These passwords, passphrases and PINS shall be designed and utilized in a manner which renders them secure and prevents unauthorized use.

Passwords, passphrases, and PINs shall be unique to the account and service for which they have been provisioned.

## Procedures

### 1. General Procedures

a) Passwords, passphrases, and personal identification numbers (PIN) shall be stored in a manner which renders them inaccessible by others.
b) Temporary passwords provided by Middlesex County ITS staff shall be changed as soon as possible upon receipt of the temporary password.
c) If a numerical personal identification number (PIN) is used to secure a system or device, the PIN shall not consist of easily guessable combinations (0000, 1234, etc.)
d) If a Password, passphrase, or PIN is known or suspected to be compromised, it shall be changed immediately.
e) “Remember Password” feature on websites and applications should not be used.
f) User IDs and Passwords/Passphrases/PINs must not be scripted to enable automatic login on workstations or laptops, except for systems designated as public-access terminals.
g) When configuring password “hints,” do not hint at the format of your password (e.g., “postal code + middle name”)

### 2. Password Managers

a) Middlesex County ITS may approve the utilization of a commercial password management system or solution for staff.
b) Approved password management systems or solutions may be local or online (cloud) based.
c) Any licensing or maintenance fees for an approved password management system or solution may be the responsibility of the department requesting access.
d) An approved/authorized password management system or solution may only be utilized provided its use does not circumvent or negate any policies or procedures outlined in this policy document.

3. **Workstations and Laptops**

   a) All Workstations and Laptops shall be secured using a password or passphrase consisting of no less than fifteen (15) characters in length.
   b) Staff passwords or passphrases utilized for Workstation and Laptop access shall be unique to the system or service being accessed and not be used for any other purpose.
   c) Staff passwords and passphrases used to access to Middlesex County Workstations or Laptops do not expire and are only required to be changed if compromised or shared per the General Procedures of this document.

4. **Servers, Firewalls, and Core Infrastructure**

   a) Passwords and passphrases used to access Servers, Firewalls and other devices defined as Core Infrastructure shall be stored in an approved Privileged Access Management System (PAM).
   b) Passwords and passphrases stored in an approved PAM shall only be accessible to Middlesex County ITS staff who have been granted access.
   **c)** Passwords and passphrases stored in an approved PAM shall be updated on a regular basis.

5. **Password Protection**

   a) Passwords or passphrases shall not be shared with anyone (including coworkers and supervisors) and must not be revealed or sent electronically.
   b) If a password, passphrase, or PIN must be shared through the course of day-to-day activities, such as granting temporary access of a system or site, it shall be changed once access is no longer required.
   c) Passwords shall not be written down or physically stored anywhere in the office.

6. **Mobile Devices**

   a) Mobile devices shall be secured using a password, PIN, or Biometric Security (or a combination thereof), as defined in the Cellphone and Mobile Device Policy (IT Policy 5.01).

## 7. Compliance

Middlesex County ITS enforces this Policy and related standards. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the Middlesex County ITS Service Desk. Policy violations that come to the attention of the ITS Service Desk will be escalated to the Director of ITS.

Staff in violation of this policy may be subject to disciplinary action up to and including termination.