Passwords

Objective:	To provide guidance and outline requirements for secure user account passwords.	**Policy/Procedure Number:**	*07-10*
Reference: *(All applicable federal, state, and local laws)*	Health Insurance Portability and Accountability Act of 1996 (HIPAA); Office of the NYS Comptroller, Information Technology Governance Local Government Management Guide; NYS Civil Service Law, Section 75	**Effective Date:**	*August 6, 2024*
		Responsible Department:	*Information Technology*
Legislative Policy Statement:	A robust password policy, complemented by the implementation of two-factor authentication (2FA), forms a critical part of an organization's security controls. Given that the user is responsible for creating strong passwords, it is imperative to have a policy that is both comprehensive and easily comprehensible.	**Modified Date (s):**	
		Resolution No.:	*2024-155*
		Next Scheduled Review:	*August 2029*

General Information:

The goals of this security policy are to accomplish the following:

1. To allow for the confidentiality and privacy of Tompkins County's information.
2. To provide protection for the integrity of Tompkins County's information.
3. To provide availability of Tompkins County's information.

This is commonly referred to as the "CIA Triad" of Confidentiality, Integrity, and Availability, an approach which is shared by all major security regulations and standards. Additionally, this approach is consistent with currently accepted industry best practices for security management.

I. Definitions:

Account - A set of privileges assigned to a user, usually defined by a username and password.

Authentication - A security method used to verify the identity of a user and authorize access to a system or network.

Biometrics - The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Confidential Data - Expressly included, but not limited to this category are ePHI and PII.

Electronic Protected Health Information (ePHI) - Defined in HIPAA regulations as any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media and includes any personally identifiable health or healthcare information that can be linked to an individual. Identifiers include social security numbers, names, addresses, and health information.

Email - Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within the County or between users of County email accounts and non-County users.

Guest - A visitor to County premises who is not an employee (includes clients, contractors, consultants, and temporary workers).

Network - Two or more computers or devices linked to each other that enable communication and sharing of their resources, data, and applications.

Password - A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Personally Identifiable Information (PII) - Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

PII references data within Criminal Justice Information - Information (CJI, or sometimes referred to as CJIS - Criminal Justice Information System) and includes sensitive information gathered by local, state, and federal law enforcement agencies. It includes criminal history records, fingerprints, copies of private documents, and other personal data.

Smart Card - A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

Token - A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

Two Factor Authentication (2FA) - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

II. Policy:

A. This policy shall apply to every person who is provided an account on the County's network or systems, including: employees, legislators, guests, contractors, partners, vendors, etc.

B. The County shall set user passwords to expire within a timeframe that the Information Technology Services (ITS) deems necessary based on industry best practices.

C. The County shall require two-factor authentication (such as authenticator applications, smart cards, tokens, or biometrics in combination with a password) on many systems, in addition to strong passwords.

III. Procedure:

A. Construction

Tompkins County mandates that users adhere to the following requirements on password construction:

- Passwords must be at least 14 characters for County hosted resources;
- Passwords must be comprised of a mix of letters, numbers and special characters (e.g. !@#$);

- Passwords must be comprised of a mix of upper and lower-case characters;
- Passwords must not be comprised of an obvious keyboard sequence (i.e., qwerty);
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.;
- Password changes should not duplicate the previous 12 passwords used;
- Passwords must not contain the username; and
- Passwords must be changed at least once per year and more often if required.

B. Confidentiality

Passwords are considered confidential data and treated with the same discretion as any of the County's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

1. Users must not disclose their passwords to anyone;
2. Users must not share their passwords with others (coworkers, supervisors, family, etc.);
3. Users must not write down their passwords and leave them unsecured;
4. Users must limit the use of the same password for different systems unless single sign-on or MFA technologies are utilized; and
5. Users must not send passwords via email.

C. Change Frequency

To maintain good security, passwords must be periodically changed. This limits the damage an attacker can do as well as helps to frustrate and slow brute force attempts to access the County’s networks.

1. At a minimum, users must change passwords at least annually; and
2. When selecting a new password, users should select a password that is substantially different than the previous password.

D. Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user’s responsibility to immediately report any suspicious activity involving their passwords to the Director of Information Technology Services. Any request for passwords over the phone or email, whether the request came from organization personnel or not, must be expediently reported. When a password is suspected to have been compromised the Director of Information Technology Services will request that the user, or users, change their password(s).

E. Enforcement

This policy will be enforced by the Department Head/Supervising Authority. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment, subject to applicable laws and collective bargaining agreements. Where illegal activities or theft of County property (physical or intellectual) are suspected, the County may report such

activities to the applicable authorities, including Federal, State, or local law enforcement agencies.