Remote Access to Information Technology Resources

Objective:	To provide standards for accessing County information technology resources from outside the County network.	**Policy/Procedure Number:**	*07-07*
Reference: *(All applicable federal, state, and local laws)*	NYS Civil Service Law Section 75; Health Insurance Portability and Accountability Act of 1996 (HIPAA)	**Effective Date:**	*November 19, 2024*
		Responsible Department:	*Information Technology*
Legislative Policy Statement:	It is often necessary to provide access to County information resources to employees or others working outside Tompkins County's Network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.	**Modified Date (s):**	
		Resolution No.:	*2024-256*
		Next Scheduled Review:	*November 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. Any specific regulations (industry, governmental, legal, etc.) relating to County use or retention of email communications must be appended to this policy.

The scope of this policy covers all employees, contractors, and external parties that access County resources over a third-party network, whether such access is performed with County-provided or non-County-provided equipment. This includes access for any reason from the employee's home, remote working locations, while traveling, etc.

I. Definitions:

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

Approved User - A County employee authorized by their Department Head to use or access devices or the County network via VPN.

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) - 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.

Firewall - A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Modem - A hardware device that allows a computer to send and receive digital information over a telephone line.

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 CJI references data within Criminal Justice - 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.

Remote Access - The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

Remote Access VPN - A VPN implementation at the individual user level. Used to provide remote and traveling users secure network access.

Remote Desktop Access - Remote control software that allows users to connect to, interact with and control a computer over the Internet just as if they were sitting in front of that computer.

Split Tunneling - A method of accessing a local network and a public network, such as the Internet, using the same connection.

Strong Encryption - Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices.

Third-Party Connection - A direct connection to a party external to Tompkins County. Examples of third-party connections include connections to customers, vendors, partners, or suppliers.

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.

Virtual Private Network (VPN) - A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

II. Policy:

A. Non-County provided computers are not allowed to access the County Network for any reason, unless the access is provided by Tompkins County in a public manner, such as web-based email.

B. Remote access to County systems is only to be offered through a County-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a County system without the written pre-approval of the Director of Information Technology Services;
- Remotely accessing County systems with a remote desktop tool, such as Citrix, or GoToMyPC without written pre-approval from the Director of Information Technology Services;
- Use of non-County-provided remote access software;
- Split Tunneling to connect to an insecure network in addition to the County Network, or to bypass security restrictions; or
- Copying data to, and storing data on, remote computers unless explicitly authorized to do so for a defined business need and done in a manner that meets requirements for data confidentiality.

C. Department Heads or their designee shall be responsible for enforcing this policy and the procedure below. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment, in compliance with Civil Service Law Section 75.

D. Where illegal activities or theft of County property (physical or intellectual) are suspected, the County may report such activities to any applicable legal authorities.

III. Procedure:

A. Remote Access Client Software

1. If determined by a Department Head that there is a departmental need for an employee to have remote access, the Department Head shall submit an *"Account Management Form"* to ITS authorizing such access. Department Heads and employees

shall consider *Administrative Policy 03-21: Telework Arrangements* as part of this determination.

2. Tompkins County Department of Information Technology Services (ITS) will supply approved users with approved devices with remote access software that allows for secure access and enforces the remote access policy. The software will provide strong traffic encryption to protect the data during transmission.

3. Further, Tompkins County ITS will provide remote users with client firewall software that will protect the remote computer when it connects directly to the Internet. This software will be configured in a consistent County-standard manner and will not be altered by the user.

B. Remote Network Access

Tompkins County requires that remote access be offered according to the level of access required by each user type, as specified below. Department Heads shall indicate the level of access required for an employee by submitting the Account Management Form to ITS. ITS Shall be responsible for providing and setting up such accesses.

1. Employees

a. Due to the elevated risks associated with remote access, two-factor authentication (such as authenticator applications, smart cards, tokens, or biometrics in combination with a password) will be implemented for VPN access when feasible.

b. Tompkins County will limit remote users' access privileges to only those information assets that are reasonable and necessary to perform their job function when working remotely (i.e., email).

2. Administrators

a. Strong passwords are required, and passwords must follow guidelines in this document for secure password construction. Refer to *Administrative Policy 07-10: Passwords* for further guidance.

b. Any non-console administrative access, such as remote management or web-based access, must be secured to prevent misuse. If such access is allowed, it must meet the following criteria:

- Remote administrative access must be encrypted using strong encryption that is initiated prior to the administrative password being requested; and

- Insecure management protocols, such as telnet, must be disabled or prohibited in favor of more secure methods, such as SSH, or encrypted via a VPN or SSL/TLS.

3. *Third Parties / Vendors*

    a. When non-employees are provided access to the network, such as vendors or service providers, their remote access account must be approved by the Director of ITS with security controls in place.

    b. Due to the elevated risk of remote access, two-factor authentication is required of vendors accessing the Tompkins County Network.

    c. Accounts used for remote vendor access can be monitored when in use when deemed necessary by the County.

C. Idle Connections

Due to the security risks associated with remote network access, idle connections will be timed out periodically. Idle remote connections to Tompkins County's network using the VPN will be timed out by ITS at their discretion and appropriate compensating controls.

D. Applicability of Other Policies

This document is part of Tompkins County's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

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, in compliance with any applicable laws and collective bargaining agreements. Where illegal activities or theft of County property (physical or intellectual) are suspected, Tompkins County may report such activities to the applicable authorities, including Federal, State, or local law enforcement agencies.