Mobile Devices

Objective:	To specify County standards for the use and security of mobile devices.	**Policy/Procedure Number:**	*07-09*
Reference: *(All applicable federal, state, and local laws)*	Health Insurance Portability and Accountability Act of 1996 (HIPAA); NYS Civil Service Law, Section 75	**Effective Date:**	*August 6, 2024*
		Responsible Department:	*Information Technology*
Legislative Policy Statement:	Mobile devices are vital tools to the workforce and sensitive data is often stored on them, and the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.	**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:

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.

Encryption - The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

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.

Mobile Device - A portable device that can be used for certain applications and data storage, such as a smartphone.

Personally Identifiable Information (PII) - Information that 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 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.

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

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.

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

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.

Wireless Access Point - A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

II. Policy:

A. This policy concerns the security of County data stored on mobile devices, including, but not limited to, laptops, notebooks, tablet computers, smartphones, and USB drives. The policy applies to both County-issued mobile devices as well as personal mobile devices accessing County data.

III. Procedure:

A. General Guidelines

The following guidelines apply to the use of mobile devices:

1. Any County-provided mobile device must directly connect to the Tompkins County Network at least once per month;

2. Loss, theft, or other security incident related to a County-provided mobile device must be reported immediately using the *"Reporting a Security Breach"* form found on the County Compliance Program web page;

3. Confidential data must not be stored on mobile devices unless explicitly authorized for a defined business need. If confidential data is stored on a mobile device, it must be appropriately secured with encryption and comply with the Confidential Data Policy;

4. Data on mobile devices must be securely disposed of in accordance with the Confidential Data Policy; and

5. Users should never store confidential data on non-County-provided mobile equipment.

B. Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. Keeping mobile devices physically secure is the first line of security defense. Therefore County staff must carefully consider the physical security of mobile devices and take appropriate protective measures including, but not limited to, the following:

1. Care must be given when using or transporting mobile devices in busy areas;

2. As a rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

3. Mobile Data Terminals (MDT's) mounted in Law Enforcement/First Responder vehicles should be screen locked when exiting the vehicle.

4. For departments that store confidential information on mobile devices, the department head must consult with the ITS Department to evaluate the data that will be stored and consider implementing remote wipe/remote delete technology. This technology enables users or administrators to render data on a mobile device unrecoverable in the event of theft or loss.

5. The ITS Department shall continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

6. To ensure equitable access to secure technology, the ITS department will provide training and resources to all county staff on best practices for mobile device security. This includes ensuring that security measures are accessible and practical for employees across all departments, regardless of their technical proficiency or resources. These measures apply exclusively to county-issued devices.

C. Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting County data. The following sections specify Tompkins County's requirements for data security on mobile devices:

1. *Laptops or Mobile Computers*

    a. County data must be stored on an encrypted partition, which is the responsibility of the County IT department to manage; whole disk encryption should be considered if the data on the device is especially sensitive.

    b. Laptops must require a username and password or biometrics for login.

    c. Two-factor authentication for login may be implemented when feasible.

2. *Smartphones/Tablets*

    Encryption and/or login passwords/passcodes are required on any smartphones or tablet computers, County provided or personally owned, if the smartphone or tablet is used to access, review, or store County data.

3. *Removable Media*

    This section applies to any USB drive, flash drive, memory stick or other removable data storage media that could be connected to County systems.

    a. If approved and provided by the Tompkins County Department of Information Technology Services (ITS), any confidential County data stored on these devices must be encrypted using strong encryption, managed by the County IT department.

    b. County data is never to be stored on personal (non-County-provided) removable media.

    c. Prior to removable media being redeployed, ITS must ensure that no previously stored confidential data can be accessed. This should be done by wiping the media with the strongest commercially available data wiping software.

4. *Other Mobile Devices*

    Unless specifically addressed by this policy, storing County data on other mobile devices, or connecting such devices to County systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the Director of Information Technology Services.

D. Connecting Mobile Computers to Unsecured Networks

1. Users must not connect to any outside network without a secure, up-to-date software firewall and antivirus/anti-malware applications configured by Tompkins County ITS on the mobile computer. Examples of unsecured networks include home networks, hotel-provided access, convention networks, or any network not under

direct control of the County.

2. Users should be particularly cautious when connecting to public hotspots. Ensure that the connection is to the intended wireless access point and not a malicious mobile hotspot. For example, while at Starbucks, connect to a network named "Starbucks Guest" rather than a network named "Sally's iPhone."

E. Audits

Tompkins County ITS must conduct periodic reviews to ensure policy compliance. ITS shall be responsible for keeping inventory of County issued mobile devices. The audit must involve the inventory and inspection of each mobile device to ensure compliance with County security policies. These inventories are to occur on a yearly basis at a minimum.

F. Applicability of Other Policies

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

G. 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 Civil Service Law, Section 75. Where illegal activities or theft of County property (physical or intellectual) are suspected, the County may report such activities to the applicable authorities.