The Administrative Manual: The Policies and Procedures of Tompkins County Government

Confidential Data

Policy/Procedure Number:	*07-06*
Effective Date:	*November 19, 2024*
Responsible Department:	*Information Technology*
Modified Date (s):	
Resolution No.:	*2024-255*
Next Scheduled Review:	*November 2029*

Objective: To lay out standards for the classification and use of confidential data and outline specific security controls to protect this data.

Reference:
(All applicable federal, state, and local laws)
NYS Civil Service Law, Section 75; NYS Office of Information Technology Services, Policies, Standards and Guidelines

Legislative Policy Statement: Confidential data can carry greater risk than general County data. Federal and State regulations/industry standards specify how certain types of data must be treated. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data. This policy covers all County-confidential data, regardless of location, including electronic and hard copies of data or information, such as printouts, faxes, notes, etc.

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:

Access Control List - A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

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.

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 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.

Disclosure - The release of, transfer to, access to, or the divulging in any other manner of protected health information to an entity or individual outside Tompkins County.

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 Storage Media - A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

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.

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.

II. Policy:

A. The County shall classify data according to its importance to County operations and the confidentiality of its contents. Once classified, the County can take steps to ensure that data is maintained, secured, and destructed appropriately. ITS will work with Department Heads to ensure understanding and classify data appropriately to align with Data Classification standards.

B. Confidential data must be identified, catalogued, and secured in all forms (i.e. electronic, printed, or stored on digital media). Confidential data shall be segregated from the County's non-confidential data so that access can be tightly controlled and tracked.

C. The County must determine the access control capabilities of each system housing confidential data to ensure that County and regulatory standards are met. When applicable, the County must acquire and implement additional hardware or software to ensure compliance.

D. The County shall create, retain, and dispose of classified data in accordance with the provisions of *Administrative Policy 11-05: Retention and Disposition of Records* and all applicable Federal, State, and Local laws.

III. Procedure: **A. Data Classification**

Departments should refer to the "NYS Office of Information Technology Services Information Classification Standards" to conduct classification of data within their department. Data types that have classifications mandated (due to applicable laws, regulations or contracts) and those that are in common use throughout the County are included.

B. Confidential Data

The following list is not intended to be exhaustive but shall provide the County with guidelines on what type of information is typically considered confidential. Confidential data may include:

- Electronic Protected Health Information (ePHI);
- Personally Identifiable Information (PII);
- Medical and healthcare information;
- Credit card information;
- Employee or customer social security numbers, or other personal information;
- Customer data, including customer lists and customer contact information;
- County financial data which has not been released publicly;
- Network diagrams and security configurations;
- Communications about County legal matters;
- Passwords;
- Bank account information and routing numbers;
- Payroll information; and
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information and append that agreement, or a summary thereof, to this policy).

C. Inventory

1. The County Information Technology Services Department, in conjunction with County Departments as needed, must identify all systems, devices, and media that house, collect, store, and process confidential data.
2. For each system identified, the County shall determine and document functions that exist on that system, determine and document ownership, responsibility, and functions of the system.
3. Remote access devices and removable media must be included in the inventory if they meet the criteria above.

D. Treatment of Confidential Data

The following sections detail County requirements on the storage, transmission, and destruction of confidential data:

1. Storage

a. Confidential electronic data should only be stored when necessary and must be encrypted whenever possible, using strong encryption methods. The County’s OneDrive and County hosted servers are encrypted by ITS.

b. Confidential data must never be stored on non-County-provided systems or devices.

c. Confidential information, whether in physical or electronic form, must be removed from desks, computer screens, and common areas when not in use, and hard copies must be stored in a secure, locked location when not actively being used.

2. Transmission

To protect data from interception or alteration during transmission, ITS will ensure the following measures are in place:

- Identify Risks of Data Interception: ITS will identify and review scenarios where confidential data may be intercepted or altered during transmission.

- Develop and Implement Transmission Security Procedures: ITS will establish and implement a set of written procedures to ensure the security of confidential data during transmission. An example would be using 'encrypt' in the subject line of an email message.

- Develop and Implement Integrity Controls: ITS will implement processes to ensure data integrity is maintained throughout the transmission process, as determined by the Director of Information Technology Services.

- Implement Encryption: ITS will ensure that weaker encryption schemes are disabled for users. For example, ITS will enforce HTTPS and display it in the browser URL bar whenever confidential data is transmitted.

3. Data Destruction

a. Media containing confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross-cut shredding or incineration is required to make the data unrecoverable.

- Storage media (CDs, DVDs): physical destruction is required, via any means that makes the data unrecoverable.

- Hard Drives/Systems/Mobile Storage Media: The strongest commercially available data wiping technology must be used to ensure that the data is unrecoverable. Alternatively, physical destruction, such that the data storage mechanism is destroyed, is an option. Departments must consult with ITS prior to wiping or destructing data or equipment.

b. Media awaiting destruction under this policy must be physically secured until the necessary destruction can take place. This can be in the form of a locked cabinet or other locked and secure storage solution.

E. Use of Confidential Data

The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data to which they are been granted access. Such data must be marked or otherwise designated "confidential."

- Users must only access confidential data when it is necessary to perform their job function.

- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.

- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do their job or the action is approved by their Supervising Authority.

- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her Supervising Authority. Refer to *Administrative Policy 11-47: Breach Incident Response* for further information.

F. Sharing Confidential Data

1. If confidential data is shared with third parties, such as service providers or Business Associates, a written confidential information, business associates agreement (BAA), and/or non-disclosure agreement must govern the provider’s use of confidential information. Further, Tompkins County must maintain a written agreement with the provider that indicates how the data will be used, secured, and destroyed.

2. When the County is sharing confidential data with a service provider or other third party, due diligence must always be performed prior to selecting the provider. Due diligence may include, but is not limited to:

i. **Evaluating the provider's security policies and protocols** to ensure they meet or exceed the County's data protection standards.
ii. **Reviewing the provider's history of handling confidential information** and their record of data breaches, if any.
iii. **Conducting background checks and verifying references** from other clients to assess the provider's reliability and trustworthiness.
iv. **Ensuring the provider has relevant certifications or compliance with legal regulations** such as HIPAA, GDPR, or other industry standards as applicable.
v. **Assessing the provider's capacity for data encryption, secure storage, and data transfer practices** to protect confidential information during and after the engagement.
vi. **Reviewing the provider's incident response and data breach notification procedures** to ensure they align with the County's expectations in case of a data breach or other security event.

3. If media containing confidential or ePHI is sent external to the County, rigorous security procedures must be developed and maintained, which will include, at minimum, credential-verification, and signature of the backup service courier. Media must be sent via a delivery method that allows the media to be tracked (i.e., USPS, UPS, FedEx, etc.), such as with a tracking number, and records the signature of the receiver.

G.Security Controls for Confidential Data

Confidential data requires additional security controls to ensure its integrity. Tompkins County requires that the following guidelines are followed:

- Strong Encryption: Strong encryption must be used for confidential data transmitted external from the County. For example, when sending an email users must type “encrypt” in the subject line of the message to ensure encryption. Confidential data should be stored whenever feasible in encrypted form, whether such storage occurs on a user system, server, laptop, or any other device that allows for data storage. See the Encryption Policy for more information about strong encryption.

- Network Segmentation: The County must use firewalls, access control lists, or other security controls to separate the confidential data from the rest of the County Network, and more specifically, to isolate confidential data where feasible. More detailed information about this can be found in the Network Security Policy section on Network Compartmentalization.

- Physical Security: Systems that contain confidential data, as well as confidential data in hardcopy form, must be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data. Refer to the Physical Security Policy for further guidance.

- Printing: When printing confidential data, the user must make their best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be in secured areas.

- Faxing: When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes must be set to print a confirmation page after a fax is sent; and the user must attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be in secured areas.

- Emailing: Confidential data must not be emailed outside the County without the use of strong encryption. More information can be found in *Administrative Policy 07-08: Email Policy.*

- Mailing: If confidential information is sent via interoffice or postal mail, data must be transported in sealed security envelopes marked "confidential."

- Wireless Access: When confidential data is transmitted or accessed via wireless networks, the County must use wireless industry best practices for encryption. Only the strongest encryption algorithms must be used to secure this data during transmission.

- Discussion: When confidential information is discussed, it must be done in non-public places, and where the discussion cannot be overheard.

- Display: When confidential data is numerical, such as social security numbers, it must be removed if possible. If necessary for this information to be displayed, it must be masked (i.e., such that only the last four digits are displayed). Please note that this restriction does not apply to employees who must have access to this data to perform their job functions. If confidential data is written on a whiteboard or other physical presentation tool, the data must be thoroughly erased after the meeting is concluded.

- Media: Any media containing confidential data must be physically secured in an access-controlled area or high security zone.

H. 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.

I. 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, Tompkins County may report such activities to the applicable authorities.