Email Policy

Objective:	Reduce risk of email-related security incidents, foster good business communications, and provide for consistent and professional application of the County's email principles.	**Policy/Procedure Number:**	*07-08*
		Effective Date:	*November 19, 2024*
Reference: *(All applicable federal, state, and local laws)*	Health Insurance Portability and Accountability Act of 1996 (HIPAA); NYS Public Officers Law, Freedom of Information Law (FOIL), Article 6, Sections 84-90; NYS Civil Service Law, Section 75	**Responsible Department:**	*Information Technology*
		Modified Date (s):	
Legislative Policy Statement:	This policy details Tompkins County's ("the County") usage guidelines for the email system. The scope of this policy includes the County's email system in its entirety, web-based email/client applications, server-side applications, email relays, and associated hardware. It covers all County provided electronic mail sent from the system, as well as any external email accounts accessed from the County Network.	**Resolution No.:**	*2024-260*
		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.

I. Definitions:

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

Backup - To copy data to a second location, solely for the purpose of safe keeping of that data.

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 and CJI references within Criminal Justice data – Criminal Justice Information (CJI, or sometimes referred to as CJIS - Criminal Justice Information System) including 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.

Data Leakage - Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with honest intentions.

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

Email - Short for electronic mail, email refers to electronic letters and other communications 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.

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

Phishing - Phishing is a type of cyber-attack in which attackers attempt to deceive individuals into providing sensitive information, such as usernames, passwords, credit card numbers, or other personal details. This is typically done by masquerading as a trustworthy entity in electronic communications.

Spam - is defined as unsolicited, bulk messages sent over the internet, typically for advertising, phishing, or spreading malware. These messages are often irrelevant or inappropriate, and they include misleading information, promotional content, or malicious links. Spam can appear in emails, social media posts, comments, text messages, and voice calls.

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. The County reserves the right to monitor all use of County email networks which may include, but is not limited to, interception and review of any email, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

B. The County owns and maintains all legal rights to its email systems and networks, and thus any email passing through these systems may be subject to use for purposes not anticipated by the user including disclosure of records in response to requests made

pursuant to the New York Freedom of Information Law ("FOIL"). County email may be backed up, or otherwise copied, retained, or used for legal, disciplinary, or other reasons. Email sent to or from certain public or governmental entities may be considered public record.

C. Usage of County email systems should be strictly limited to conducting County business. Personal email must be sent from personal email accounts on personal devices. The County email system is for County communications only, excepting occasional incidental use for personal purposes (such as communicating revised transportation arrangements to a child during inclement weather).

D. Users of County email systems are expected to check and respond to email in a consistent and timely manner during County business hours.

E. Email signatures (contact information appended to the bottom of each outgoing email) shall be inserted for all email sent from the County email system. Email signatures must not include personal messages (political, humorous, etc.) and must be professional in nature.

F. Email disclaimers shall be included on every outgoing email.

G. Mass email may be used when communicating with County employees or constituent base. The sending of spam is strictly prohibited.

H. Users must use the County email system for all business-related email. Users are prohibited from sending business email from a non-County-provided email account.

I. Any email containing confidential information, regardless of whether the recipient is internal or external to the County Network, must be encrypted.

J. Copies of this policy will be distributed to all new employees by the Human Resources Department at the time of hire and will be available to all employees in the Administrative Policy Manual on the County website.

K. Department Heads and/or Supervisors shall be responsible for insuring that this policy is implemented and adhered to within the County department(s) which they are responsible.

L. Email will be retained and backed up in accordance with the applicable County policies which may include, but are not limited to, the following: 07-06: Confidential Data and/or NYS Archives, Retention and Disposition Schedule for NYS Local Government Records (LGS-1).

III. Procedure: **A. Proper Use of County Email Systems**

The following applies to the proper use of the County's email system.

1. Sending Email

When using a County email account, email must be addressed and sent carefully. Once an email is sent externally from the County's networks, the County loses any control of the email. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists to avoid inadvertent information disclosure to an unintended recipient(s).

2. Business Communications and Email

Email sent from a County account reflects on the County, and, as such, email must be used with professionalism and courtesy. Employees shall check with their supervisor for any additional requirements for e-mail communications unique to the department.

3. Email Signature

An email signature shall include the user's:

- Name;
- Department;
- Title;
- Phone number(s);
- Fax number, if applicable; and
- URL for County website.

4. Out-of-Office Reply

Tompkins County recommends the use of an out-of-office reply if the user is out of the office for an entire business day or more. The reply should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.

5. Mass Emailing

Tompkins County makes the distinction between the sending of mass email and the sending of unsolicited bulk email (spam). It is the County's intention to comply with applicable laws governing the sending of mass email and to be consistent with good business practices. Email sent to more than twenty-five (25) external recipients should have the following characteristics:

- The email must contain a subject line relevant to the content;
- The email must contain sender or return contact information; and

- The email must not contain intentionally misleading information (including the email header), blind redirects, or deceptive links.

Note: Email sent to County employees are exempt from the above requirements.

6. Opening Attachments

a. Users must use extreme care when opening email attachments. Malware, phishing, and cyber security threats can be easily delivered as an email attachment. Users must:

- Never open unexpected email attachments;
- Never open email attachments from unknown sources; and
- Never click links within email messages unless you are certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially formatted email can hide a malicious URL.

b. The County may use methods to block what it considers to be dangerous email or strip potentially harmful email attachments as it deems necessary.

7. Contents of Received Email

If unsolicited or spam email becomes a problem, the County may attempt to reduce the amount of this type of email that users receive. The best course of action is to not open email(s) that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, they can report the message using the County's Phishing Alert Button (PAB). If the user believes that it contains illegal content, they must notify their supervisor immediately.

8. Access to Email from Mobile Devices

While it is not encouraged, users are permitted to access their email on personal devices. However, it is important to be aware of the security concerns associated with checking county email on personal devices, such as increased risk of data breaches and unauthorized access.

B. Confidential Data and Email

1. Passwords

As with any County passwords, passwords used to access email accounts must be kept confidential and used in adherence with County *Administrative Policy 07-10: Password Policy*. At the discretion of the Director of Information Technology Services (ITS), the County may further secure email with certificates, two-factor authentication, or other security tools.

2. Emailing Confidential Data

Guidance on confidential information can be found in Tompkins County *Administrative Policy 07-06: Confidential Data*.

C. County Administration of Email

Tompkins County will use its best effort to administer the County's email system in a manner that allows the user to both be productive as well as reduce the risk of an email-related security incident.

1. Filtering of Email

a. Tompkins County may choose to filter email before it reaches the user at the internet gateway and/or the mail server. The purpose is to filter out spam, viruses, or other messages that may be deemed a potential risk to the County's IT security. No method of filtering email is 100% effective.

b. Additionally, many email and/or anti-malware programs will identify and quarantine email that it deems suspicious. This functionality may be used at the discretion of the Director of Information Technology Services.

2. Email Disclaimer

The use of an email disclaimer, which is text appended to the end of every outgoing email message, is an important component in the County's risk reduction efforts.

a. The approved disclaimer is:

"CONFIDENTIAL NOTICE

This transmission, including any attachments, is for the sole use of the intended recipient(s) or entity named above and may contain confidential and privileged information. If you received this and are not the intended recipient(s), you are hereby notified that any disclosure, copying, unauthorized distribution or the taking of any action in reliance on the contents of this information is prohibited. If you received this transmission in error, please immediately contact the sender to arrange the proper handling of the information."

b. The ITS Department must periodically review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all required information. If information has been changed or updated, ITS will notify users of the County email system and will update this policy accordingly.

3. Email Deletion

a. Users are encouraged to delete email periodically when the email is no longer needed for business purposes. This will

assist in keeping the size of the user's email account manageable and reduce the burden on the County to store and backup unnecessary email messages.

b. Users are strictly forbidden from deleting email to hide a violation of this or any other County policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

4. Address Format

Email addresses must be constructed in a County approved standard format to maintain consistency across Tompkins County.

Tompkins County can choose any format if it can be applied consistently throughout the organization. The intent of this policy is to simplify email communication as well as provide a professional appearance.

5. Email Aliases

Often the use of an email alias, which is a generic County email address that forwards email to a user account, is recommended when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for County email, as well as (often) the names of County employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

6. Email Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive County email.

a. Accounts will be set up at the time a new hire starts at the request of the hiring department, or when a promotion or change in work responsibilities for an existing employee creates the need for email access via the submission of an *"Account Management Form"*.

b. Contractors may be assigned temporary email accounts in situations where necessary. Contractor accounts must be monitored and deleted as soon as the need for the account has ended.

7. Email Account Termination

a. When a user leaves County employment, or their email access is officially terminated for another reason, the user's department supervisor must complete the Account Management form requesting ITS to disable the user's access to the account by password change or another method.

b. Please note that the County is under no obligation to block the account from receiving email and may continue to

forward inbound email sent to that account to another user or set up an auto-response to notify the sender that the user is no longer employed by the County.

8. Storage Limits

Email storage may be provided on County servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the Director of Information Technology Services. Storage limits may vary by employee or position within the County.

D. Prohibited Actions

The following actions shall constitute unacceptable use of the County email system. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the County email system to:

1. Send any information that is illegal under applicable local, State, or Federal laws or regulations;

2. Send email without proper encryption when required;

3. Access another user's email account without:

    a. the knowledge or permission of that user – which should only occur in extreme circumstances; or
    b. the approval of County Department Heads and/or their designee in the case of an investigation; or
    c. when such access constitutes a function of the employee's normal job responsibilities.

4. Send any unauthorized email about County business in an employee's official capacity that may cause embarrassment, damage to reputation, or other harm to the County (*see Administrative Policy 01-40: Public Statements about County Business*);

5. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene, pornographic, or otherwise inappropriate messages or media;

6. Send email that causes disruption to the workplace environment. This includes sending email that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere;

7. Send email that may be construed as an act or as part of a pattern or series of acts that constitute unlawful discrimination, retaliation, or sexual or other harassment [add reference in heading of policy for sexual harassment, general harassment, and anti-discrimination policies];

8. Make fraudulent offers for products or services;

9. Attempt to impersonate another person or forge an email header;

10. Send spam, solicitations, chain letters, or pyramid schemes;

11. Knowingly misrepresent the County's capabilities, business practices, warranties, pricing, or policies; or

12. Conduct non-County-related business, except for occasional incidental use for personal purposes (such as communicating revised transportation arrangements to a child during inclement weather).

E. Data Leakage

Data can leave the network in several ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a challenge to Tompkins County's control of its data.

Unauthorized emailing of County data, confidential or otherwise, to external email accounts for the purpose of saving this data external to County systems is prohibited.

Tompkins County may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the Director of Information Technology Services.

F. Sending Large Email

Email systems were not designed to transfer large files; email(s) should not contain attachments of excessive file size larger than 25 MB.

G. Legal Rights Not Impaired

Nothing contained in this Policy shall be deemed to limit or impair an employee's ability to engage in communications allowed or required by law to report unlawful activity or misconduct, including the exercise of rights pursuant to Civil Service Law §75-b, the Taylor Law, or any other Federal, State or local law, or pursuant to the collective bargaining agreement covering the employee's terms and conditions of employment.

H. 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.