Acceptable Use of County Information Technology Resources

Objective:

To establish guidelines for acceptable use of the following County Information Technology (IT) resources:

- Computers, computer workstations, laptops, tablets, other end-user devices and network resources;
- E-mail;
- Internet; and
- Telephone and voice-mail system.

Policy/Procedure Number: *07-01*

Effective Date: *September 2, 2014*

Responsible Department: *ITS*

Modified Date (s):

Resolution No.: *2014-169*

Next Scheduled Review: *September 2019*

Reference:
(All applicable federal, state, and local laws)

Tompkins County Code of Ethics (as amended by Local Law No. 2, July 16, 2013); NYS Public Officers Law, Article 6, Sections 84-90; Administrative policies 08-06 (Public Access to Records),11-05 (Retention and Disposition of Records),09-21 (Surplus Equipment), and 02-13 (Disciplinary Action or Discharge Procedure); NYS Arts & Cultural Affairs Law.

Legislative Policy Statement:

Information Technology (IT) resources owned, leased, or maintained by Tompkins County and data contained therein are the property of Tompkins County government and shall be used to support legitimate County business purposes. The use of these resources imposes certain responsibilities and obligations on County officers or employees and other authorized users and is subject to Tompkins County policies and applicable local, state, and federal laws.

General Information:

This policy applies to all County officers or employees and other authorized users including County legislators and elected officials, contractors, interns, advisory board members, and visitors having access to the County network and other IT services owned, leased, or managed by the County. County officers or employees and other authorized users are responsible for using these resources in a professional, lawful, and ethical manner.

Although County officers or employees and other authorized users are expected to maintain the privacy and confidentiality of information to which they have access, users are not guaranteed personal privacy of any data and information, or for any activity in which they use County computing or telephone resources. All data and account audit details managed on IT systems owned or leased by Tompkins County may be disclosed pursuant to New York State Freedom of Information Law (FOIL), public disclosure laws, and rules of discovery in the event of lawsuits or other legal actions.

Departments have the ability to define additional or enhanced Information Technology Acceptable Use policies and procedures beyond the scope of those defined in this policy (such as those required by governing state and federal authorities). These enhancements must be documented by the Department Head and reviewed by the Director of Information Technology Services (ITS) and the County Administrator.

Acceptable use and prohibited use of County information technology systems and resources are actively monitored and users should have no expectation of privacy in their use of these systems and resources. Identified abuse of computing and telephone resources may result in disciplinary action.

I. Definitions:

Board - Refers to the Tompkins County Legislature or any County administrative board, commission, or other agencies or body of the County of Tompkins.

Confidential Information - Includes any information that would (i) affect current or imminent contract awards or collective bargaining negotiations, or (ii) interfere with law enforcement investigations or judicial proceedings, or (iii) deprive a person of his/her right to a fair trial or impartial adjudication, or (iv) constitute an unwarranted

invasion of privacy, or (v) endanger the life or safety of any person, or (vi) provide civil service examination questions or answers prior to administration of the examination, or (vii) reveal computer access codes, or (viii) provide any information that is specified as non-disclosable by federal or state law. Confidential information also includes procedures that determine whether other information is confidential as described in the Tompkins County Administrative Policy Manual.

County Officer or Employee - A paid or unpaid officer or staff member of Tompkins County, including, but not limited to, the members of any County board.

Data Encryption - The process of transforming electronic information into a scrambled form that can only be read by an individual who has the appropriate tools and/or password to translate the code.

E-Discovery - Refers to any process in which electronic data are sought, located, secured, and searched with the intent of using them as evidence in a civil or criminal legal case.

NYS Freedom of Information Law (FOIL) - Gives the public the right to access, with certain exceptions, documents and information about the functions, procedures, policies, decisions and operations of County government departments and agencies.

Personal Health Information (PHI) - Any information that relates to the health of an individual, the provision of care to an individual, or the payment for the provision of health care to an individual that identifies the individual and is transmitted or maintained by the County.

Private Information (PI) - Personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- Social security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

II. Policy:

This policy provides a common standard for the appropriate use of County information technology (IT) resources to support productivity and to facilitate efficiencies in meeting daily operations and County business needs. The policy also guides prudent and responsible use in response to regulatory compliance and data security requirements.

The IT resources covered by this policy include:

- All **computers, computer workstations, laptops, tablets, other end-user devices, and network resources** managed by Tompkins County ITS, or connected to the Tompkins County data network.
- All **Internet access**, services and data owned, leased, and/or provided by Tompkins County and all systems and associated data supported by Tompkins County ITS related to the management and utilization of internet access.

- All **e-mail systems and services** owned by Tompkins County and/or managed by Tompkins County ITS, including County e-mail account users, and all records and information stored at any point in time within the County's e-mail system.
- All **telephone and voice-mail systems and services** owned or leased by Tompkins County and/or managed by Tompkins County ITS and all records and information stored at any point in time within the County's telephone and voice-mail systems.

The Director of ITS, in consultation with the County Administrator or the Commissioner of Personnel, has the authority to revoke an individual's account access based on a determination of inappropriate use (see Section E) or a need to respond to known IT security issues related to any IT resources covered under this policy. Upon determination by the Director of ITS and the County Administrator or the Commissioner of Personnel, that the identified IT issue has been mitigated, access may be subsequently restored.

A. Computers, Computer Workstations, Laptops, Tablets, Other End-user Devices, and Network Resources

1. Computer equipment will not be removed from Tompkins County premises without either prior written authorization from the Department Head or alternative established department procedures. All computer equipment when removed from Tompkins County premises must be used for the purpose of conducting County business.

2. All computer equipment and peripheral storage devices that contain confidential information, PI, or PHI, must be configured with encryption provided by ITS prior to removal from Tompkins County premises.

3. Other than County business software, officers or employees shall not install or store software without prior written authorization from Tompkins County ITS.

4. ITS does not provide data backup services for data stored locally (C:/ or D:/ drives) on computers, computer workstations, laptops, tablets, or other end-user devices. The use of external internet storage services or directly attached storage devices as means of primary data storage is not permitted without prior written authorization from the Department Head and the Director of ITS.

5. Data not related to County business should not be stored on any Tompkins County computer equipment or other network resource. Tompkins County ITS will not be responsible for personal data or data not related to County business.

6. A user ID and password shall be required for all computers, computer workstations, laptops, tablets, and other end-user devices owned or managed by Tompkins County.

7. All computers, computer workstations, laptops, tablets, and other end-user devices when not in use during non-working hours must be completely shutdown. Network logoff, hibernate, and standby do not qualify as a complete shutdown.

B. Internet Access

1. All Tompkins County officers or employees are eligible to receive internet access unless otherwise stated in writing by their respective Department Head.

2. User-level access to internet services and web sites is granted based on individual and County business requirements. County ITS, in consultation with the respective Department Head, has the authority to determine and implement the appropriate level of internet access for users.

3. Temporary internet access for non-County employees or non-authorized users must be coordinated through County ITS.

4. To ensure security standards, Tompkins County ITS is authorized to access, monitor, block, and capture any internet traffic or data passing through or maintained within the County IT system(s).

5. Limited personal use of the internet is permitted so long as it does not interfere with staff productivity, pre-empt any County policy or County business activity, compromise IT security requirements, consume more than an acceptable amount of IT resources (such as bandwidth), or is not listed as a prohibited use in Section E of this Policy.

C. E-mail

1. All officers and employees of Tompkins County are eligible to receive an e-mail account, unless otherwise stated in writing by their respective Department Head.

2. When conducting County-related business via e-mail, officers or employees and other authorized users must use e-mail system(s) provided by the County or approved via written authorization by the County Administrator and the Director of ITS that shall require a commitment by the user to transfer to the County e-mail system all e-mails that deal with County business.

3. E-mail access at Tompkins County is controlled through individual accounts and

passwords. It is the responsibility of the individual to protect the confidentiality of his or her account and password information. Each user is responsible for the content of all e-mail, including attachments sent from an individual user's account or an account for which he/she may have additional responsibility.

4. All data or information residing or originating on County e-mail systems are the sole property of Tompkins County and are not considered personal or private.

5. All e-mail sent or received via the Tompkins County e-mail system is archived and may be subject to public access via FOIL and e-discovery requests. Therefore, the Tompkins County e-mail system shall be used to support legitimate County business purposes only. If an officer or employee receives e-mail messages personal in nature it shall be the responsibility of the officer or employee to communicate to the sender an alternate personal e-mail address.

6. Archival and backup copies of e-mail messages and content exist in compliance with Tompkins County's records retention practices despite deletion by an individual e-mail user. Backup and archiving procedures are to ensure system and data reliability, provide for retrieval of historical e-mail account content and information, and to meet regulatory requirements and respond to potential e-discovery and FOIL requests.

7. E-mail that contains confidential information, PI, PHI, and information protected by New York state or federal law shall not be transmitted without proper encryption.

8. E-mail distribution lists maintained by the ITS Department must be used to only support County business.

9. E-mail access will be removed when the individual's association with Tompkins County is terminated, unless other arrangements are authorized by the Director of ITS. Tompkins County is under no obligation to provide copies of, forward or maintain any content associated with an individual's e-mail account after the term of employment or elected County term of office has ceased.

10. The Director of ITS has the authority to establish best practices for e-mail account management, which may result in limitation of e-mail attachment and mailbox size.

D. Telephone and Voice-mail

1. Limited personal use of County telephones is allowed provided that use does not interfere with staff productivity, pre-empt any County policy or County business activity, or consume more than an acceptable amount of resources as defined by the Department Head.

2. Personal long distance, toll-based telephone calls originating from any County telecommunication equipment is prohibited unless approved by the Department Head or Supervisor. Officers or employees are required to reimburse the County for all personal long distance, toll-based telephone calls that are directly charged to the County.

3. To ensure security requirements and best practice, Tompkins County ITS has the authority to monitor, filter, capture, and access any call data detail passing through or maintained within its telephone and voice-mail system(s).

E. Prohibited Use and Failure to Comply

Tompkins County officers or employees and other authorized users shall at all times refrain from using County IT resources for prohibited use. Prohibited use is subject to disciplinary action up to and including termination of employment or contractual agreement. Prohibited uses include but are not limited to the following illustrative list:

- Conducting private or personal for-profit or unauthorized not-for-profit activities;
- Conducting any political solicitations (see Tompkins County Code of Ethics);
- Conducting any solicitation for any purpose except those officially

sanctioned by Tompkins County;

- Conducting any unlawful activities as defined by federal, state, or local law, regulation, or policy;
- Producing, accessing, displaying, or transmitting sexually explicit, indecent, offensive, harassing or intimidating material, such as pornography or racial epithets, that could reasonably be considered threatening, offensive, intimidating, or discriminatory;
- Producing, accessing, or participating in online gambling;
- Attempting to modify or remove computer equipment, components, software, or peripherals without written authorization from the Department Head and Director of ITS;
- Attempting to subvert the security of the Tompkins County network or network resources;
- Downloading, installing, or running software that reveal or create weaknesses in the security of the Tompkins County network or network resources;
- Accessing, copying, modifying, or deleting files, data, accounts, and access rights for applications or system functions without written authorization from the Department Head and Director of ITS;
- Disclosing confidential, PI, PHI, or otherwise non-public data and information without following appropriate regulatory and/or department-specific disclosure processes;
- Breaking into systems and databases or acting to disrupt the functioning of systems or causing unnecessary computing disruption.
- Using Tompkins County IT resources to engage in acts that unfairly monopolize IT resources for personal use to the exclusion of others. This includes streaming media (such as use of Hulu, Pandora, or Netflix) for personal use.

F. Special Requests for Access to or Monitoring of Another User's ITS Accounts

III. Procedure:

Requests for access to or monitoring of another employee's or authorized user's ITS resources that are covered by this policy and that are owned, maintained, or leased by Tompkins County government, such as e-mail account, voice-mail account, internet use activities, or county software systems must be submitted in writing to the Director of ITS. There are no time-based restrictions on such requests. The employee or authorized user assigned to the accounts may or may not be notified of such requests for access or monitoring or of the outcome of such requests.

Authorizations and Approvals

1. A Department Head or elected official may submit such a monitoring request only for the account(s) of an employee or authorized user accounts under his/her direct authority.

2. Based on the nature of the request, the Director of ITS may consult the County Administrator and /or County Attorney for additional approvals, as needed.

A. Lost or Stolen Computing Equipment

Any computing equipment that is lost or stolen must be reported to ITS and the Department Head.

B. E-mail

Misuse
Any allegations of e-mail system(s) misuse should be promptly reported to the appropriate Supervisor, Department Head, or Director of ITS. Any user who receives an offensive e-mail, must not forward, delete, or reply to the message, but instead, report it directly to one of the individuals named above
.
Mailbox Maintenance
Individuals should remove all non-critical e-mail communications and attached files.

Temporary Accounts
Temporary e-mail accounts may be granted to non-County employees and other authorized users on a case-by-case basis. Requests for temporary accounts must be submitted to and approved by the Director of ITS. All terms, conditions, and restrictions governing the temporary e-mail account by non-County employees or other authorized users must be in the form of a written and signed agreement.

C. Allegations of Misuse

Any allegations of misuse should be promptly reported to the appropriate Supervisor, Department Head, Director of ITS, or to the County Compliance Officer.

D. Password Requirements - Microsoft Active Directory (network access, email, Office 365)

Passwords are an important component of information and network security. The use of a Network- ID and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is met.
The minimal requirements for Microsoft Active Directory passwords are as follows:

- At least eight characters in length, and a maximum of 16 characters in length.
- At least one upper case letter, one lower case letter, one number, and one non-alphanumeric character (!, $, #, %).
- The same password, or a like password (Example: Da!sy1234 change to Da!sy12345), cannot be reused within the previous 12 password resets.
- The forced change of Active Directory passwords will occur every 90 days.
- A password can only be reset once within a 24-hour period without assistance from ITS.
- Passwords cannot contain a users' name (Suzy Smith) and users' account name (ssmith).

E. Acknowledgement

Officers or employees and other authorized users must acknowledge that they have read the policy governing Acceptable Use of County Information Technology Resources and agree to abide by the policy guidelines. The officer or employee and authorized user understand that if he or she has questions, at any time, regarding the policy, he or she will consult with the designated supervisor or

Department Head.