SECTION VIII – COMPREHENSIVE INFORMATION SECURITY POLICY
(FORMERLY POLICY #44)

Tioga County, New York

Comprehensive Information Security Policy

Policies, Procedures, and Standards for Information Security

I. Contents

II. Purpose

The purpose of the Tioga County Comprehensive Information Security Policy is to protect the confidentiality, integrity, and availability of all information that County Agencies, towns and villages and employees, create, receive, maintain or transmit.

It is to provide a security framework that will ensure the protection of Tioga County information from unauthorized access, loss or damage while supporting the open, and information-sharing needs of our county. This information may be verbal, digital, and/or hardcopy, individually-controlled or shared, stand-alone or networked. Failure to comply with this policy may subject you to disciplinary action up to and including termination.

This document is organized by audience to assist in clearly defining the responsibilities required for different roles.

III. General Provisions

A. Definitions

- **Breach**
  A security incident, in which sensitive protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
- **Business Associates**
  Is an organization or individual that performs services for a covered entity (healthcare organization) that has access to protected health information (PHI).

- **Chief Information Officer**
  An individual named by the County Legislature who has the responsibility for establishing and maintaining all Information Systems within the County.
- **Confidential Data**
  Protected information that is not available to the general public.
- **Covered Entities**
  Any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR).
- **Data Custodian**
  The individual or group who has responsibility for maintaining the tools necessary for storing of data by the data owners. Ex: ITCS maintains servers that a department's software program runs on. ITCS is the data custodian as the maintainer of the server\data storage infrastructure.
- **Data Owner**
  The individual who is responsible for the maintenance and safekeeping of data, whether it be electronic or physical.
- **End User**
  Individuals performing work for Tioga County, whether they are employees or contractors.
- **Deputy Director of ITCS**
  An individual named by the County Legislature to function as a point person for ensuring compliance with the details of this policy.
- **Phishing**
  The attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication (email, website etc.).
- **Protected Health Information (PHI)**
  Any information in a medical record that can be used to identify an individual.
- **Public Data**
  Information that may be freely disseminated is considered to be *public* data. However, even though the data may be freely disseminated to the public, the integrity of the data must be protected.
- **Ransomware**
  A type of malware that restricts access to an infected computer system in some way and demands that the user pays a ransom to the malware operators to remove the restriction.
- **Spear Phishing**
  An email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information.
- **Social Engineering**
  The art of manipulating people so they give up confidential information.
- **Super Users**
  Users who are granted additional authority for specific functions on the data network.

B. Breach Policy for High-Risk and Confidential Data

Any breach of High-Risk and Confidential Data must be reported to your supervisor who will report it to the Deputy Director of ITCS and the County Attorney immediately for investigation. The County Attorney and Deputy Director of ITCS shall investigate the matter and recommend further action to ensure compliance with applicable statutory requirements and County Policy provisions.

C. Facility Security Plan

Access to every office, computer room, and work area containing High-Risk or Confidential information will be physically restricted.

Visitors and other third parties must not be permitted to use employee entrances or other uncontrolled pathways leading to or through areas containing High-Risk or Confidential information.

Identification badges, keys and physical access cards that have been lost or stolen – or are suspected of being lost or stolen – must be reported to the Department Head or designee, who will notify Buildings and Grounds, or any other appropriate entity, immediately. Likewise, all computer or communication system access tokens that have been lost or stolen – or are suspected of being lost or stolen – must be reported to the Department Head or supervisor and Deputy Director of ITCS immediately. All Personal approved devices lost or stolen that contain Tioga County data must also be reported to the Department Head or supervisor and Deputy Director of ITCS immediately.

Each person must present his or her badge to the badge reader before entering every controlled door within Tioga County premises. Before proceeding through every controlled door, each person must wait until the reader indicates that they have permission to enter the area. Workers must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances.

Whenever controlled doors are propped open (perhaps for moving supplies, furniture, etc.) the entrance must be continuously monitored by an employee or guard.

Tioga County employees must not attempt to enter restricted areas in Tioga County buildings for which they have not received access authorization.

D. Contingency Operations

In the event that primary facility access controls are not functional or unable to be utilized, the Buildings and Grounds department shall keep as part of the County's Disaster Plan the backup or secondary methods for facilities access. This includes consideration for ensuring data is secured in the event a primary security control (e.g. electronic door lock) is non-operational.

E. Data Security Policy

County Information Assets shall be handled in accordance with their Data Classification and in accordance with appropriate federal and state statutes and regulations.

Tioga County employees may be in a position to receive confidential information during the performance of their duties. County employees shall never use information obtained confidentially for any non-business-related purpose and shall respect the privacy of the data according to its classification. Since public access of information varies, employees should consult with their supervisor/Department Head regarding the dissemination of High-Risk or Confidential information. Violations of this confidentiality requirement may be grounds for disciplinary action, up to and including termination.

F. Data Classification Policy

It is essential that all County data be protected. However, there are gradations that require different levels of security. All data should be reviewed on a periodic basis by the Data Owner and classified according to its use, sensitivity, and importance. Tioga County recognizes four classes of data: Public, Internal, Confidential, and Restricted Use.

Public Classification is any data that may be disclosed to the public. An example may be an announcement or general information.

Internal Classification is sensitive information that is not shared with the public. An example may be some memos, contact lists and procedures.

Confidential Classification is secure data that needs protection. This data would have limited access. An example may be HIPAA data.

Restricted Use Classification is highly sensitive information and should be limited on a need-to-know basis. An example of this would be passwords.

Data Owners and their supervisors must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

IV. Audience – Legislature

A. General

The Legislature holds responsibility to adopt any changes to the Information Security Policy as necessary and create and appoint members as necessary to a Data Disaster Recovery Workgroup.

B. Evaluation

The Tioga County Legislature shall receive, review, and adopt the following:

- External Risk Assessment Report every two years (Section VII)
- Risk Mitigation and Management Plan every two years (Section VII)

- Disaster Testing and Revision Analysis annually (Section VII.F)
- Data Criticality Analysis annually (Section VI.G)

V. Audience – End User

A. Sanction Policy

Failure to comply with any of the policies contained in this document may result in disciplinary action up to and including termination of employment.

B. Expectation of Privacy

All County information resources, including but not limited to equipment, documents, data, information, records and software are the property of Tioga County. Users have no expectation of privacy in their use of County computer and information resources. County equipment, data, records, software and connections are County property, provided for County purposes only. Software and systems that can monitor use may be used. Use of County computer systems and networks constitutes consent to such monitoring.

C. Intellectual Property - Legal Ownership

With the exception of material clearly owned by third parties, Tioga County is the legal owner of all business information stored on or passing through its systems. Unless a specific written agreement has been signed with the Legislature, all business-related information, including but not limited to copyrights and patents, developed while a user is employed by Tioga County is Tioga County property.

D. Passwords

Passwords will be changed once every calendar year. They will be at least twelve characters long. There will be a history of eight (8). Which means the end user will not be able to use the same password for 8 calendar years.

E. Acceptable Use - General

It is the user's responsibility to utilize Information and Information Technology resources appropriately and ensure their security. Users shall not use County Information or County IT systems for purposes other than those that support official County business or as defined in this policy.

Except when in the process of conducting law enforcement activities, users shall not use County IT systems to intentionally obtain or generate information containing content that may be reasonably considered offensive or disruptive. Offensive content includes, but is not limited to images, or comments of a sexual nature, racial slurs, gender offensive comments, or any comments that would offend someone on the basis of age, sexual orientation, gender identity, religious or political beliefs, national origin, or disability.

The provisions, terms, and rules for acceptable use apply to the use of all County systems and equipment whether in a County Building, remote site, or when working from home or any other location using County resources.

Incidental personal use of any of the below listed tools is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any business activity. Users are forbidden from using Tioga County electronic communications systems for charitable endeavors, political campaigns, private business activities, or amusement/entertainment purposes. The use of County resources, including electronic communications should never create either the appearance or the reality of inappropriate use.

F. Acceptable Use – e-mail

As a productivity enhancement tool, Tioga County encourages the business use of electronic communications. Electronic communications systems, including backup copies, are considered to be the property of Tioga County. Tioga County cannot guarantee that e-mail communications will be private. All e-mail communications may be stored and archived by ITCS for 7 years. E-mail messages are considered to be "documents" and are subject to all statutory and legal compliance, particularly in reference to Schedule LGS-1 published by the New York State Archives. E-mail items that are not "official documents" as described by the New York State Archives should be deleted as soon as they are no longer needed. E-mail items that do fit the definition of "official documents" should be stored in a permanent archive or other appropriate medium for the period of time defined by regulation or statute. See your department's record officer for more information on this.

Sending high or moderate risk information outside of our County email system must be encrypted. This is done by selecting the ENCRYPT icon at the top of the Outlook NEW EMAIL screen or by selecting Options then ENCRYPT, if using Office 365.

County employees are prohibited from using personal e-mail to conduct County business.

It is the responsibility of the individual user to manage and maintain their e-mail mailbox. ITCS may employ quotas on mailbox size to enforce compliance. Messages no longer needed for business purposes must be periodically purged by users from their email system mailbox. After a certain period – generally six months – e-mail messages stored on the email server may be automatically archived by ITCS staff.

It is the policy of Tioga County not to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored, and the usage of electronic communications systems will be monitored to support operations, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that Tioga County will from time to time examine the content of electronic communications.

It may be necessary for ITCS personnel to review the content of an individual employee's communications during the course of problem resolution. ITCS personnel may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is forbidden. The username, e-mail address, organizational affiliation, and related information included with e-mail messages or postings must reflect the actual originator of the messages or postings.

Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, constituents, or others. Such remarks may create legal problems such as libel and defamation of character.

Message Forwarding: Some information is intended for specific individuals and may not be appropriate for general distribution. Users should exercise caution when forwarding messages. Tioga County High-Risk and Confidential information must never be forwarded to any party outside the County unless the message is encrypted and/or Department Head approval has been obtained.

G. Acceptable Use – Internet

All Internet users are expected to be familiar with and comply with this policy. Violations of this policy can lead to revocation of system privileges and/or disciplinary action up to and including termination. Tioga County users have no expectation of privacy in Internet usage.

Access to the internet will be provided to those Tioga County employees who have need for such access for the performance of their official County duties. Upon recommendation of the Department Head, users may be granted either unrestricted or restricted access to the Internet. Should a user require unrestricted access, ITCS must be informed in writing, by the Department Head, in either a service ticket or e-mail.

Tioga County employees should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers must not send information over the Internet if it is classified as High-Risk or Confidential information.

Tioga County routinely logs websites visited, files downloaded, time spent on the Internet, and related information. Department Heads may receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

Tioga County routinely uses technology to prevent users from connecting to certain non-business web sites. Workers using Tioga County computers who discover they have connected with an inappropriate web site that contains sexually explicit, racist, violent, or other potentially offensive material must

immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that users of Tioga County systems are permitted to visit that web site.

Tioga County strongly supports strict adherence to Intellectual Property rights, copyright law, and software vendors' license agreements. Download and use of copyrighted software in a manner that violates the license agreement and without permission are prohibited. Tioga County employees should assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" as well as specific information about the source of the information (author names, URL's dates, etc.). Reproduction, forwarding, or in any other way republishing or redistributing words, graphics, or other materials must be done only with the written permission of the author/owner.

H. Acceptable Use – VPN (Virtual Private Network) or Other Remote Access

VPN access may be provided to employees, contractors, business partners, and members of other agencies based on demonstrated need and job function as approved by the Department Head. VPN Access is to be used only to support County government business and all the general provisions of the General Acceptable Use policy stated above apply to all VPN use. VPN Access will be granted by ITCS upon written memo from the Department Head. Employees may be granted VPN access during business hours if they are working from a remote site, such as a school or conference.

I. Acceptable Use – Cellular Phones and Other Wireless Devices

Tioga County may provide employees with cell phones, smart phones and other appropriate mobile and wireless devices, when necessary for the performance of their County duties.

Cellular phone service, like other means of communication, is provided for the sole purpose of supporting County business operations

Employees are required to reimburse the County for personal use. Employees must understand that unreimbursed personal use of County Cell Phones may be audited by the IRS and be reportable as income.

Employees shall not use cellular telephones for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interest of Tioga County.

Department Heads must review all cellular telephone statements for compliance with this policy. Any use not in accordance with this policy may result in disciplinary action, up to and including termination of employment, in addition to reimbursement to the County for all costs associated with non-compliance.

Cellular phones or other mobile devices shall not be used while operating a motor vehicle.

Smartphones and other mobile devices will be password protected.

J. Working from Home or Other Remote Sites

The scope of this section does not indicate working from home is authorized for any particular employee, and only discusses the precautions and steps that must be employed if authorization is given or allowed through a separate policy.

Laptop computers and mobile devices such as tablets, smart phones or other devices, hereafter referred to as mobile devices, as well as Remote Desktop access services may be provided to employees based on demonstrated need and job function as approved by the Department Head. This includes but is not limited to employees whose positions involve on-call duties, employees who during the normal course of employment perform their duties away from their assigned workspace, and employees who have demonstrated a need to be in contact with their office via email and other communication interfaces. County business should always be conducted on County-issued computers or devices approved for use by ITCS. Users should never use personal computers to conduct County business except through County authorized tools or mechanisms.

Mobile devices, like other means of communication, are to be used only to support County government business. Employees may use mobile devices to communicate outside of the County government when such communications are related to legitimate business activities and are within their job assignments or responsibilities.

Employees shall not use mobile devices for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of Tioga County.

User identification and passwords must be enabled and used on all Mobile devices and mobile computing devices in accordance with County policy. Access codes must be protected and will be required to be changed in accordance with Tioga County's Password Policy. Mobile devices will be either turned off or locked when not in use.

Users shall avoid leaving mobile devices in situations that increase the risk of theft and never leave mobile devices unattended or unsecured. If the mobile device is stolen, you must immediately report this to your supervisor who will inform the appropriate Department Head, ITCS and appropriate law enforcement authorities.

Mobile devices will not be used while operating a motor vehicle. Employees must take every effort to ensure the safe usage of mobile devices.

Employees must take every effort to ensure the security, safety and maintenance of the mobile device. Any unreasonable use, abuse, neglect, or alterations of mobile device equipment may result in the loss of computing privileges. Misuse of mobile devices will result in appropriate disciplinary action up to and including termination of employment.

Users are required to immediately report any problems with their mobile devices to Information Technology Helpdesk at extension 8294. Any attempt by employees to dismantle or repair their machines or to install modifications themselves may invalidate the manufacturer's warranty.

It is mandatory for all County users of mobile devices to copy or move all data files stored on the hard drives to the network so they will be backed up according to the critical nature of the data. It is the policy of the County that no user or County data be stored on mobile devices, and instead be stored and accessed from County servers. An exception shall be made for circumstances such as travel outside the County network where access to specific local files is necessary (e.g. presentation on mobile device for out of area court appearance.) Upon return, the user must delete those locally stored files from the computer.

No personal hardware or software is allowed to be loaded on the Mobile Device. All equipment and software of any kind is the sole property of Tioga County.

Failure to comply with this policy may result in discipline, up to and including termination.

K. Remote Office Security

Before approval for working at home or telecommuting is granted, a user's Department Head must review the security environment of the proposed working environment through employee interview or onsite evaluation. If the user works with sensitive information, a shredder must be employed. If sensitive information will be stored in paper form, locking furniture or a safe must be available. Users must also make sure they are connected to VPN when saving their files or at least saving documents in their assigned OneDrive.

The security of Tioga County information and physical property at remote locations is just as important as it is in the office. All the same security requirements apply at remote locations, although they may be implemented in different ways. For example, paper-based Confidential and High-Risk information must be locked up when not in active use. In Tioga County offices, a file cabinet might be used, but on the road, or at home, a locking briefcase might be employed.

L. Handling of Sensitive Information

In general, sensitive (Confidential, High or Moderate Risk) information, regardless of whether it is in paper or electronic form, should not leave Tioga County offices. If it is necessary to remove sensitive information from Tioga County offices - e.g., a court hearing - this information must be protected as appropriate for the type of media. Sensitive data may only be removed from County premises when it is encrypted and securely locked.

M. Security Incident Reporting Procedure

Users shall report all suspicious activities, social engineering attempts, anomalous behavior of equipment, systems or persons, virus activity, and any unusual occurrences to their department supervisor immediately. The department supervisor shall report this information to the ITCS Department and the County Deputy Director of ITCS at the time of the reported incident. The ITCS Department will conduct an investigation as required by the nature of the incident and will document their findings and report back to the department supervisor within ten business days. ITCS and the Deputy Director of ITCS will contact law enforcement agencies if their investigation warrants it.

N. Workstation Security

1. General

Workstations are a gateway to secure network storage, printing, applications and other services. Data shall never be stored on individual workstations. Workstations are not backed up and may be removed, replaced or erased and reconfigured at any time by ITCS without prior notice. End users are responsible for ensuring that all data resides on appropriate network resources and that no data is stored on their individual computer. All data must be stored on either Home Folders, Shared Folders, or other applicable network storage devices.

No network devices, including but not limited to computers, hubs, switches and routers, and wireless devices shall be attached to the Tioga County network unless they have been approved in writing by the CIO. Moreover, only members of the ITCS Department or approved contractors may attach network devices to the Tioga County Network. Users may not bring workstations or other devices from home and attach them to the network unless approved in writing by the CIO or designee. The CIO or designee reserves the right to revoke personal device access to the network at any time.

All workstations must have county-approved virus protection software on them, configured in accordance with the current Malicious Software Policy.

Workstations shall be stored in controlled access areas, or in areas where there is minimal probability of unauthorized personnel viewing screens or data. When workstations must be stored in public areas, screens shall be

turned away from public view. When this precaution is not possible, covers will be installed in order to preclude passerby access to High-Risk and Confidential information. When a user leaves his or her work area or office for any period of time, the user must place the desktop in a password-protected "locked" state. Any devices found left in "Logged in" state must be reported to the Deputy Director of ITCS and Department Head.

2. Removable Media

Considering federal and state regulations on information security, use of rewritable media including but not limited to flash drives, cell phones, diskettes, DVDs and CDs is strongly discouraged. Users shall not utilize personal removable media devices in County computer systems.

Media not intended for redistribution must be formatted before being discarded according to applicable regulations.

Connecting Cell phones via USB on any Tioga County Technology device is strictly prohibited unless written permission from the CIO or designee has been granted.

3. Media Disposal

Media containing County Information Assets, including but not limited to floppy disks, CDs, hard drives, flash drives, cell phones and other removable media will be treated in accordance with applicable state and federal statute or regulation. When media is no longer required, it will be turned over to ITCS for proper disposal.

Hard drives from workstations must go through a certified, approved destruction process. ITCS shall document and maintain a record of receipt and disposition and will provide copies to the responsible parties.

4. Media Reuse

If media is to be reused or redistributed, the user or ITCS must repartition and format the media. If a department has determined a need for the use of rewritable media and the media is coming from a source outside the County network, the media must be scanned for malware prior to using any information on the media.

5. Data Backup and Storage

Before being edited, or before performing upgrades, or before moving County equipment that holds County data, all data shall be backed up in order to create and preserve a retrievable, exact copy of the data.

O. Printing

When users are printing High, Moderate risk or Confidential data they shall take precautions to ensure that their privacy and security are protected. Examples of this include:

- Stand by the printer while the job is printing.
- Immediately remove the documents from the printer.
- Print to a printer/copier mailbox and release the print job when standing at the printer/copier.
- Print to a printer/copier in a secure area.
- Lock file cabinets and records rooms that contain High-Risk and Confidential Data when unattended and/or during non-business hours.

P. Data Restoration

End users who require restoration of data shall inform their supervisor and the ITCS Department immediately. They will provide ITCS with as much information about the data, including the location and the approximate date and time of deletion. Depending on the circumstances, the data may or may not be available for restoration.

VI. Audience – Department Heads \ Supervisors

A. Authorization and Supervision

Department Heads are responsible for the authorization and supervision of employees who work with High and Moderate Risk or Confidential information within their departments. Department Heads must ensure that the relevant procedures described in this policy are followed in order to mitigate the risk of unauthorized use or release of High and Moderate Risk or Confidential Data.

B. Workforce Clearance Procedures

The County shall conduct background checks, of the following current and prospective County employees:

- All full-time and part-time employees, except elected officials and employees of the Tioga County Board of Elections, hired after 1/1/2016.
- All temporary and seasonal employees, except employees of the Tioga County Board of Elections, hired after 1/1/2016 who may have access to High-Risk or Confidential Information.
- All current employees of the Personnel and ITCS Departments, except employees hired before 1/1/2016 who are represented by CSEA.

Nothing in subparagraph (1) above shall preclude a Department Head from conducting such other background checks of current and prospective County employees as may be required by law or internal department policy.

C. Termination \ Separation Procedures

The Department Head shall notify the Personnel Office when an employee is to be terminated or otherwise separated from County employment. Upon receipt of such notification, the Personnel Office shall notify ITCS. ITCS shall secure the employee's data by whatever means necessary and appropriate under the circumstances, including moving the data, locking or deleting the employee's system accounts, redirecting or deleting the employee's phone extension and

voice mail, and/or securing or deleting the employee's email box. The Department Head may request specific actions be taken via a service ticket. The Department Head must make sure all assigned equipment is returned to the department and verified with the ITCS Department. Any approved Personal Devices will immediately lose access to the county network and data.

D. Access Authorization, Establishment & Modification

The access authorization process for employees and contractors will be initiated by an employee's department in a service ticket or e-mail describing the level of access, group membership, and other appropriate information needed to grant access. Authorization will be granted by the Department Head or alternatively by the CIO. The privileges granted remain in effect until the worker's job changes or the worker leaves Tioga County, or until the department otherwise notifies ITCS of a change. If any of these events takes place, the Department Head must immediately notify the ITCS Department.

E. Departmental Security Training

Each County Department is required to hold, at a minimum, annual training for their users concerning the management of Information Security. It is the responsibility of the individual Department Head to ensure that this training takes place and records are maintained concerning the scope of the training as well as documentation of those employees that attended the training.

ITCS shall sponsor Countywide annual security training for the County Staff that employees are required to complete once per calendar year. Attendance at this training can be used as proof of compliance with the departmental security training requirements.

F. Business Associate Agreement

All Covered Entities and Business Associates (as the terms are defined by HIPAA) within the County are required to have in place a current, HIPAA compliant Business Associates Agreement (BAA) with any and all vendors, contractors, subcontractors, consultants, non-county agencies or other service providers who are their Business Associate. The BAA must address specific compliance issues in keeping with all New York and Federal statutes, rules and regulations. Each BAA must be approved by the County Attorney prior to execution. Department Heads shall consult with the County Attorney to ascertain whether their department is a Covered Entity or Business Associate.

In some instances, County Departments are Business Associates (defined in Definitions above) of Non-County Covered Entities. In the event a County Department is asked to enter into a BAA with a Non-County Covered Entity, the BAA must be reviewed and approved by the County Attorney prior to execution.

Any County Department that is either a Covered Entity or Business Associate, as those terms are defined by HIPAA, shall maintain a current list of all BAAs entered into by their department and shall ensure that said BAAs are kept current.

It is the responsibility of the Department Head of the County Covered Entity or Business Associate to ensure that the requirements of this section are met.

G. Vendor Access Control

All Vendors requiring access to Tioga County electronic resources on the Tioga County network must be submitted for review and approval by the by the CIO or Deputy Director of ITCS. All software with Vendor service agreements, requiring access for support, must also be submitted for review and approval by the CIO or Deputy Director of ITCS. Vendors requiring continual access will use the Tioga County authorized Virtual Private Network solution.

All methods of vendor remote access must be approved by the CIO or Deputy Director of ITCS. Department Heads must contact the ITCS Department before allowing any Third-Party Access to Tioga County Network. Access will be granted only for the requested maintenance window. Once support is completed, Access will be terminated, and Vendor accounts disabled. The CIO or Deputy Director of ITCS reserves the right to disable all Vendor access at any point in time.

Vendors chosen by Department Heads must follow the same compliance requirements which that Department adheres. All vendors must comply with the Comprehensive Security Policy and be given this policy prior to signing any contracts.

H. Application Level Authentication, Logging and Integrity Controls on High-Risk Data

Individual Department Heads with applications that contain or store High-Risk data are responsible for monitoring the security and logs of their applications and must record and document these activities. All department level applications must be password protected at the user interface and must have password protection at the database and file level. Departments with such application must have a written policy on log monitoring and management and must monitor the logs on a regular basis. This responsibility may be assigned to a staff member(s) who will take responsibility for the task. Department Heads must ensure that the data has not been altered by unauthorized personnel. All the policies that apply to the County network apply to individual applications.

I. Keys and Swipe Cards

Each Department Head shall determine the level of access, via key or swipe card, that each employee within his/her department may have to County facilities within the Department Head's authority and control. NOTE: Certain County employees/contractors, such as IT, Buildings and Grounds, cleaning staff

and the Tioga County Safety Officer, are entitled to such access to County facilities as is required to perform their job functions.

Upon an employee's separation from County employment, the Department Head shall:

- collect all swipe cards and keys issued to the employee; and
- return all keys to the Buildings and Grounds Department; and
- terminate swipe card system access.

Each department shall maintain a written record of the names, dates and times of all swipe card assignments and changes in access permissions.

The Buildings and Grounds Department shall maintain a written record of the names, dates, and times of all key assignments, the changes to all locks and the repairs to all doors.

J. Solicitation

Solicitation is any form of requesting money, support or participation for products, groups, organizations or causes. Tioga County employees, contractors and volunteers are not allowed to use any electronic device, network or social media owned by Tioga County. The exception is any pre-approved solicitation such as United Way.

VII. Audience – ITCS Department

A. Data Network Configuration

1. Firewalls

All county-owned computers and networks shall be protected by a physical or virtual network firewall to prevent intrusion, theft, or breach.

2. Time Synchronization

All network devices and phones attached to the Tioga County network shall have their internal clocks synchronized with a single time source, maintained by ITCS.

3. Passwords

Passwords shall be at least 12 characters in length consisting of upper- and lower-case alphabetic characters, numbers, and punctuation characters. Where systems support it, this minimum length shall be enforced automatically. Passwords shall be changed at a minimum of every 365 days and the password history shall be maintained for the last 8 passwords.

4. Automatic Logoff & Screensavers

Screen Savers shall be configured to activate after 10 minutes of inactivity so that High-Risk and Confidential information is not visible during periods of user inactivity. System policy shall be configured to automatically log-off users after 8 hours of inactivity, when possible.

5. Login Banners

When logging in to a workstation or any other Information Systems device in Tioga County, the device will display a login banner reminding users of their responsibilities to be familiar with County Information Security Policies and of their responsibility to help maintain the security of Tioga County's information assets, if supported by the device. The banner states: *Computer Systems Access. This device is a part of the Tioga County, New York computer network. Usage of this device is governed by the Comprehensive Information Security Policy, found in Section VIII of the County Employee Handbook. Unauthorized use prohibited.*

6. Protection from Malicious Software

All Tioga County devices are required to have appropriate protection from Malware installed and configured for centralized management and reporting. Tioga County ITCS shall provide and configure network-level software and policies that monitor malware.

7. Login Monitoring

Login banners shall display Last Login information whenever a user logs into a County device when possible.

8. Server and Network Infrastructure Device Security

Servers shall be placed in locked rooms that have access limited to authorized personnel only. Administrative access to servers will be strictly limited to members of the ITCS Department, approved contractors, software vendors, and in rare cases, super users in individual departments. When possible, servers will be placed so that only ITCS members and IT contractors have access to them. Because of privacy and security requirements, users who are neither ITCS members nor approved contractors will not receive administrative-level permissions.

Server desktops shall remain logged out at all times unless a member of the ITCS staff or a contractor is working on the server. When administrative tasks are complete, the operator will log out immediately.

When remote access to servers is required, members of the ITCS Department will use only approved, encrypted communications for these sessions.

9. Server File System Security

With the exception of HOME folders, only Active Directory Domain Global Groups shall be used to apply security to server resources on Tioga County servers. Individual user objects shall never be assigned access to any folders or other shared server resources.

10. Workstation System Security

User privileges on a workstation shall be assigned at the lowest level possible. Initially, the user's workgroup shall be assigned *Domain User* access. However,

some applications will not work properly unless the user has a higher level of privileges. If this has been demonstrated to be the case, the user shall be granted the lowest level required for applications to work properly. At the discretion of the Department Head and with authorization from the CIO, users may be assigned administrative privileges to their workstations.

Workstations shall be configured to allow Remote Desktop and Virtual Network Computing (VNC) access to the workstation and shall be configured so that authorized support personnel can login in order to provide technical support.

B. Network Folder Configuration

1. Home Folders

Users who are assigned network accounts will receive a HOME directory (folder) for storage of their daily work. Only the individual user and the ITCS Department will have access to HOME folders.

2. Shared Folders

Users shall be assigned access to shared folders in accordance with departmental or workgroup requirements as directed by the user's supervisor. Shared folders are for the purpose of allowing entire workgroups or departments to share data. Requests for special workgroups or cross-departmental workgroups should be referred to the ITCS Department.

3. Application Folders

Users shall be assigned access to shared folders in accordance with departmental or workgroup requirements as directed by the user's supervisor.

C. Network Intrusion, Virus or Malicious Software Outbreak

Should a network intrusion, virus or malicious software outbreak be suspected, ITCS will take the following steps:+

- Record and Capture any necessary system information
- Backup, isolate, and shut down (if necessary) the compromised system
- Search other systems for signs of intrusion or infection
- Secure and examine logs
- Identify how the intruder gained access, if applicable
- Identify what the intruder did, if applicable
- Collect and preserve evidence
- Contact Law Enforcement (if necessary)
- Identify and implement new security features or procedures to protect from a recurrence of a similar intrusion
- Provide a report to the Deputy Director of ITCS that details the identified issue, what steps were taken to address it, and progress on eliminating the threat from the network until completion

D. Data Backup Plan

End users are responsible for ensuring that all County data is stored on county file servers. The ITCS Department is responsible for backing up and restoring data on servers and is responsible for ensuring the confidentiality, integrity, and availability of the County data that is stored on servers. To that end:

- All servers shall be fully backed up at least once a week and backup images will be maintained for at least 30 days.
- All servers shall be incrementally backed up every business day. However, daily full backups are preferred, when possible.
- At least two sets of full backups shall be maintained off-site and rotated weekly.
- An ITCS staff member shall review all server backup logs daily and will record the status of backups on a daily checklist/report.
- At least once a quarter, a member of the ITCS staff will perform a random test restoration of data from backup media in order to ensure the integrity of the backups.
- For automated backups, a backup user will be created. Backups will not be performed under the Administrator account.
- A record of backups will be kept by ITCS for review.

Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted, or disks destroyed consistent with industry best practices for the security level of the data.

E. Disaster Recovery and Emergency Mode Operation Plans

The Tioga County Emergency Management Office maintains a Countywide disaster recovery document, known as a Continuity Of Operations Plan (COOP.) The COOP plan covers key elements of physical disaster recovery operations for County departments including:

- How the department will conduct business during an emergency.
- The key resources that are required for emergency operations and enumerate how those resources will be provided.
- The backup location(s) where the department will conduct operations.
- How the department will contact key personnel in an emergency.
- How the department will disseminate information during an emergency.
- Enumerating a timeline for the reconstruction of normal operations

The ITCS Department maintains a Data Disaster Recovery Plan that addresses the following IT and data-specific disaster needs:

- Identifying the configurations of key County IT infrastructure.

- Enumerating and ranking the most likely failures or disasters that can occur.
- Documenting action plans for mitigating the identified potential disasters.

The CIO will be provided with a Countywide master key that allows access to all facilities with IT assets that may require physical access or intervention by an IT staff member.

F. Disaster Testing and Revision Procedure

Tioga County shall establish a Data Disaster Recovery Workgroup consisting of, at minimum, representative(s) from ITCS and representative(s) from the Emergency Management Office. This group shall annually conduct a review, with key departments, of the processes the County intends to follow in a disaster. This group is responsible for annual testing and review of the Data Disaster Recovery Plan no later than March 15th. A report of the testing and review, along with recommended remediation shall be presented to the County Legislature no later than June 30th. The group is responsible for ensuring that all remediation is performed no later than December 31st annually.

During testing of the Data Disaster Recovery Plan, the Data Disaster Recovery Workgroup will annually review processes and procedures taking into consideration the relative importance of critical systems and data.

G. Determining Data Criticality

Tioga County shall have a formal process for defining and identifying the criticality of its computing systems and the data contained within them. The responsibility for this process lies with the Disaster Recovery Workgroup. The prioritization of Tioga County information systems must be based on an analysis of the impact to Tioga County services, processes, and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time. The criticality analysis must be conducted with the cooperation of the Legislature, Department Heads, and owners of Tioga County information systems and business processes. The criticality analysis must be conducted as part of the annual disaster testing and revision procedures

At a minimum, this process will include:

- Creating an inventory of interdependent systems and their dependencies.
- Documenting the criticality of Tioga County's information systems (e.g. impact on users of Tioga County services).
- Identifying and documenting the impact to Tioga County services, if specific Tioga County information systems are unavailable for different periods of time (e.g. 1 hour, 1 day).
- Identifying the maximum time periods that County computing systems can be unavailable.

- Prioritizing County computing system components according to their criticality to the County's ability to function at normal levels.

H. Critical Systems, Applications and Data

1. General

During an emergency, operations and data should be restored within 72 hours.

ITCS will utilize the following classifications and definitions to identify other critical systems, application and data:

a) Safety Critical Systems & Applications (SCS)

A Safety Critical System or application is a computer, electronic or electromechanical system whose failure may cause injury or death to human beings. Downtime is unacceptable and appropriate measures, such as redundant systems are required.

During an emergency, these systems will receive the highest priority and will be restored as quickly as possible.

These systems shall maintain uptime of 99.7% or better.

b) Mission Critical Systems & Applications (MCS)

A computer, electronic, or electromechanical system whose failure would cause grave financial consequences is considered to be a *Mission Critical System or Application*. Downtime during general business operations is unacceptable. However, downtime during an emergency or disaster is acceptable if the system resumes operations within a period of 48 hours after the emergency is over.

These systems shall maintain uptime of 99% or better.

c) Core Systems & Applications (CS)

A computer, electronic, or electromechanical system whose failure would cause operational difficulties, increased workload, and inconvenience to staff and clients.

These systems shall maintain uptime of 98% or better.

d) Standard Systems and Applications (SS)

During an emergency, standard systems and applications should be restored within 96 hours.

2. Emergency Access Procedures for Critical Systems and Data

ITCS shall maintain a database of all applications in use by Tioga County employees and rate the applications according to the priority of restoration that will be required in the case of a disaster or interruption of operations.

Table of County Systems and Classifications

Type of System	System or Application
Safety Critical Systems (SCS)	911 Center Telephone Systems and Radio System
Mission Critical Systems (MCS)	I5 Series, Accounting and Financial Systems, Core Network Equipment
Core Systems (CS)	Infrastructure devices and systems
Standard Systems	County File Servers

I. Maintenance Windows

ITCS requires a maintenance window on all equipment that it maintains. The maintenance window will be in keeping with the system uptime standards. Routine maintenance will be announced and coordinated with the affected department.

J. Access Control

1. User Identification (User IDs)

Each User shall be assigned their own unique userid. This userid follows an individual as they move through the County. It shall be permanently decommissioned when a user leaves Tioga County; re-use of userids is not permitted. Userids and related passwords must not be shared with any other individual (Users should instead utilize other mechanisms for sharing information such as electronic mail, shared folders, etc.). Userids are linked to specific people, and are not associated with computer terminals, departments, or job titles. Anonymous userids (such as *guest)* are not permitted unless mitigative controls are in place.

2.Encryption

Electronic High-Risk data must be encrypted whenever being transported outside of County facilities on removable media. Protected Electronic data also must be encrypted at rest using various approved encryption methods.

K. Audit Controls

All County file servers and core network devices such as firewalls and routers shall have logging enabled and the logs shall be sent to a central log server maintained by ITCS. At a minimum, the following types of events shall be logged:

- Logon/Logoff Events
- Account Lockouts
- Logon/Logoff Exceptions
- Authority and Permission Changes
- Privilege use and elevation.

ITCS shall monitor the logs daily and will immediately report anomalous behavior to the Deputy Director of ITCS.

L. Data Transmission & Encryption Policy

High-Risk and Confidential data must be encrypted during transmission over non-secure channels, abiding by the following definitions and conditions:

- A non-secure channel is defined as any public network, including but not limited to the Internet.
- The Public Switched Telephone Network is considered to be a secure medium (i.e. faxing and telephone calls on a landline).
- Tioga County Employees are not permitted to encrypt or apply passwords to data unless it is for the purpose of transmission over a non-secured channel.

Tioga County ITCS will provide services and training to end users for the secure, encrypted transmission of data and will provide detailed documentation for these services to County employees.

M. Information Retention

County Information Assets, including archival backups, must be retained in accordance with applicable federal and state statute, including the *Retention and Disposition Schedule for New York Local Government Records (LGS-1)*. Where permitted by statute, documents will be scanned, indexed, and retained in electronic format as a substitute for original documents. Document imaging will be performed in accordance with the *New York State Archives Imaging Production Guidelines (2014)*.

N. Security Training

Annual Security Training (as referenced in section VI (E)) shall be performed by members or designees of the ITCS Department. ITCS shall maintain responsibility for the content and coordination of these training sessions each year.

O. Policy Changes

ITCS Department will notify all users, including employees and shared services, of any policy and training changes or notifications.

VIII. Audience – Deputy Director of ITCS

A. Information Security Duties of the Deputy Director of ITCS

The County shall appoint an employee who is responsible for implementing and monitoring a consistent data security program. The Deputy Director of ITCS shall:

- Report directly to the Chief Information Officer to help improve and communicate the maturity levels of information security, state of and information technology risk priorities across Tioga County networks and systems.

- Be responsible for overseeing information security, cyber security and IT risk management programs based on industry-accepted information security and risk management frameworks.
- Provide proactive identification and mitigation of IT risks as well as responding to observations identified by third party auditors or examiners.
- Review the Information Security Policy on an annual basis for both accuracy and to ensure continued HIPAA compliance. If changes in policy are necessary, those changes shall be submitted for review and approval by the Legislature with the report.
- Coordinate every two years a Risk Assessment that may be conducted by an external consultant. The Risk Assessment will review current security policies, the County's compliance therewith and identify any deficiencies. The results of the Risk Assessment will be used to create a Risk Assessment Report that shall be submitted to the Legislature for review and approval. The assessment will be conducted every two years and results will be presented to the Tioga County Legislature about twelve weeks after.
- Create a *Risk Mitigation and Management Plan* from the results of the Risk Assessment and present to the Legislature for review on or about 16 weeks from the date of the Risk Assessment. This plan will suggest remedies and solutions for deficiencies identified in the Risk Assessment. These deficiencies will be remedied, or a Legislature-approved plan prepared to address the deficiency by, on or about 24 weeks from the date of the Risk Assessment. The Deputy Director of ITCS is responsible for ensuring that risk mitigation is assigned to appropriate parties and completed within a reasonable amount of time.
- Develop and manage the frameworks, processes, tools and consultancy necessary for ITCS to properly manage risk and to make risk-based decisions related to IT activities.
- Development of periodic reports and dashboards presenting the level of control compliance and current information security risk posture.
- Participate in tabletop Emergency Response exercises as outlined in this policy.
- Work with the County Attorney to investigate information security breaches; ensure compliance with any and all reporting protocols required by the applicable statutes, rules and regulations and County policies; ensure that corrective measures and procedures to prevent, detect and contain future information security breaches are implemented. Monitor information security activities and oversee the application of specified security procedures.
- Assist personnel in assessing data to determine classification level.

- Facilitate ITCS security management education and training, including but not limited to annual cyber awareness training for all Tioga County users.