Tioga County Local Development Corporation

Investment Policy

This Investment Policy of the TCLDC shall apply to all operating funds, bond proceeds and other funds and all investment transactions involving operating funds, bond proceeds and other funds accounted for in the financial statements of the Corporation. Each investment made pursuant to this Investment Policy must be authorized by applicable law and this written Investment Policy. This Investment Policy is intended to comply with the General Municipal Law, the Public Authorities Law, and any other applicable laws of New York State.

Objectives

The primary objectives, in order of priority, of all investment activities involving the financial assets of the Corporation shall be the following:

A. Legal: to conform to all applicable federal, state and other legal requirements;

B. Safety: to adequately safeguard principal;

C. Liquidity: to provide sufficient liquidity to meet all operating requirements;

D. Return: to obtain a market rate of return.

Delegation of Authority

The responsibility for conducting investment transactions involving the Corporation resides with the Finance Committee of the Corporation under the direction and oversight of the Treasurer of the Corporation. Only the Finance Committee and those authorized by resolution or the Corporation's By-laws may invest public funds.

Prudence

All participants in the investment process shall seek to act responsibly as custodians of the public trust and shall avoid any transaction that might impair public confidence in the Corporation to govern effectively. Investments shall be made with judgment and care, under circumstances then prevailing, which persons of prudence, discretion and intelligence exercise in the management of their own affairs, not for speculation, but for investment, considering the safety of the principal as well as the probable income to be derived.

Operative Procedure

The Corporation shall conduct all of its investment activities in a manner that complies with the General Municipal Law and the Public Authorities Law of New York State. The Finance Committee shall submit to the Board of Directors

on an annual basis an investment report of the current portfolio in terms of maturity, rates of return and other features and summarize all investment transactions that have occurred over the past year.

Diversification

It is the policy of the Corporation to diversify its deposits and investments by financial institution, by investment instrument, and by maturity scheduling.

Internal Controls

It is the policy of the Corporation for all moneys collected by any officer or employee of the government to transfer those funds to the Treasurer or President within five [5] days of deposit or receipt, or within the time period specified in law, whichever is shorter. The Finance Committee is responsible for establishing and maintaining an internal control structure to provide reasonable, but not absolute, assurance that deposits and investments are safeguarded against loss from unauthorized use or deposition, that transactions are executed in accordance with management's authorization and recorded properly, and are managed in compliance with applicable laws and regulations.

Designation of Depositories

The bank or savings and loan association authorized for the deposit of moneys is any bank or savings and loan association doing business within Tioga County.

Collateralizing of Deposits

In accordance with the provisions of General Municipal Law § 10, all deposits of Corporation, including certificates of deposit and special time deposits, in excess of the amount insured under the provisions of the Federal Deposit Insurance Act shall be secured by a pledge of "eligible securities" with an aggregate "market value" as provided by GML § 10, equal to the aggregate amount of deposits from the categories designated in Appendix A to the policy.

Safekeeping and Collateralization

Eligible securities used for collateralizing deposits shall be held by a Third Party and/or bank or trust company subject to security and custodial agreements. The security agreement shall provide that eligible securities are being pledged to secure the Corporation's deposits together with agreed upon interest, if any and any costs or expenses arising out of the collection of such deposits upon default. It shall also provide the conditions under which the securities may be sold, presented for payment, substituted or released and the events which will enable the Corporation to exercise its right against the pledged securities. In the event that the securities are not registered or inscribed in the name of the Corporation, such securities shall be delivered in a form suitable for transfer or with an assignment in blank to the Corporation or its custodial bank. The custodial agreement shall provide that securities held by the bank or trust company, or agent of and custodian for, the Corporation, will be kept separate and apart from the general assets of the

custodial bank or trust company and will not, in any circumstances, be commingled with or become part of the backing for any other deposit or other liabilities. The agreement should also describe that the custodian shall confirm the receipt, substitution or release of the securities. The agreement shall provide for the frequency of revaluation of eligible securities and for the substitution of securities when a change in the rating of a security may cause ineligibility. Such agreement shall include all provisions necessary to provide the Corporation a perfected interest in the securities.

Permitted Investments

As authorized by General Municipal Law § 11, the Corporation authorizes the Finance Committee to invest moneys not required for immediate expenditure for terms not to exceed its projected cash flow needs in the following types of investments:

- Special time deposit accounts
- Certificates of deposit
- Obligations of the United States of America
- Obligations guaranteed by agencies of the United States of America where the payment of principal and interest are guaranteed by the United States of America
- Obligations of the State of New York
- Obligations issued pursuant to LFL § 24.00 or 25.00 (with approval of the State Comptroller) by any municipality, school district or district corporation other than the Corporation
- Obligations of public authorities, public housing authorities, urban renewal agencies and industrial development agencies where the general State statues governing such entities or whose specific enabling legislation authorizes such investments

All investment obligations shall be payable or redeemable at the option of the Corporation within such times as the proceeds will be needed to meet expenditures for purposes for which the moneys were provided.

Authorized Financial Institutions and Dealers

All financial institutions with which the Corporation conducts business must be credit worthy.

1. Banks may be asked to provide proof of a minimum three (3) star Bauer rating at the request of the Corporation.

2. Security dealers not affiliated with a bank shall be required to be classified as reporting dealers affiliated with the New York Federal Reserve Bank, as primary dealers.

The Finance Committee is responsible for evaluating the financial position and maintaining a listing of proposed depositaries, trading partners and custodians. In addition, the Audit Committee shall establish appropriate limits to the amount of investments which can be made with each financial institution or dealer. Such listing shall be evaluated at least annually.

Purchase of Investments

The Finance Committee, upon approval of the Board, is authorized to contract for the purchase of investments:

1. Directly, including through a repurchase agreement, from an authorized trading partner;

2. By participation in a cooperative investment program with another authorized governmental entity pursuant to Article 5G of the General Municipal Law where such program meets all the requirements set forth in the Office of the State Comptroller Opinion No. 88-46, and the specific program has been authorized by the governing board;

3. By utilizing an ongoing investment program with an authorized trading partner pursuant to a contract authorized by the governing board.

All purchased obligations, unless registered or inscribed in the name of the Corporation, shall be purchased through, delivered to and held in the custody of a bank or trust company. Such obligations shall be purchased, sold or presented for redemption or payment by such bank or trust company only in accordance with prior written authorization from the officer authorized to make the investment. All such transaction shall be confirmed in writing to the Corporation by the bank or trust company. Any obligation held in the custody of a bank or trust company shall be held pursuant to a written custodial agreement as described in General Municipal Law § 10.

The custodial agreement shall provide that securities held by the bank or trust company, as agent of and custodian for, the Corporation, will be kept separate and apart from the general assets of the custodial bank or trust company and will not, in any circumstances, be commingled with or become part of the backing for any other deposit or other liabilities. The agreement shall describe how the custodian shall confirm the receipt and release of the securities. Such agreement shall include all provisions necessary to provide the Corporation a perfected interest in the securities.

Repurchase Agreements

Repurchase agreements are authorized to the following restrictions:

- All repurchase agreements must be entered into subject to a Master Repurchase Agreement.

- Trading partners are limited to banks or trust companies authorized to do business in New York State and primary reporting dealers.
- Obligations shall be limited to obligations of the United States of America and obligations guaranteed by agencies of the United States of America.
- No substitution of securities will be allowed.
- The custodian shall be a party other than the trading partner.

Reserve Accounts

The Finance Committee shall establish and maintain according to the investment policy the reserve accounts set forth below. The intent of the reserve accounts shall be to utilize the monies allocated solely for the purposes authorized by General Municipal Law Section 854 and for the purposes stated therein. Any deviation shall require a resolution by the Board setting forth the reasons and justifications for the deviation from this reserve policy with such resolution requiring a 2/3 vote of the members of the Board to pass.

A. Infrastructure - This account shall be for upgrading or establishing new infrastructure within the County of Tioga. For purposes of this reserve account, infrastructure shall include utilities, public highways and roads, public sewer and public water systems or districts. Uses shall include, but not be limited to, feasibility studies, engineering reports and matching funds for grants. Uses shall not include the building or construction of any the infrastructures unless matching funds of at least 50% are provided by other sources.

B. Site Development - This account shall be for the development of new commercial sites. Monies in this reserve account may be used for actual site work and preparation, engineering reports and feasibility studies or matching grants.

C. Land Acquisition - This account shall be for the purchase of any privately owned real property to be used for future development. Monies from this account may also be used for any and all expenses incurred in the purchase and sale of real property. Any and all sale proceeds from the real property purchased by monies from this reserve account shall be returned to this reserve account for future land acquisition.

D. General Fund - This account shall be used for the general administrative purposes of the Corporation.

This Investment Policy shall be reviewed and approved annually.

APPENDIX A

Schedule of Eligible Securities

Obligations issued, or fully insured or guaranteed as to the payment of principal and interest, by the United States of America, a Corporation thereof or a United States government sponsored corporation.
Obligations issued or fully insured or guaranteed by the State of New York, obligations issued by a municipal corporation, school district or district corporation of such State or obligations of any public benefit corporation, except the TCLDC, which under a specific State statute may be accepted as security for deposit of public moneys.

Obligations of counties, cities and other governmental entities of a state other than the State of New York having the power to levy taxes that are backed by the full faith and credit of such governmental entity and rated in one of the three highest rating categories by at least one nationally recognized statistical rating organization.

Obligations of domestic corporations rated in one of the two highest rating categories by at least one nationally recognized statistical rating organization.

Any mortgage related securities, as defined in the Securities Exchange Act of 1934, as amended, which may be purchased by banks under the limitations established by bank regulatory agencies.

As well as any other financial investment that may be appropriate and deemed eligible by General Municipal Law.

Adopted 09/03/08 Revised 11/04/09

Tioga County Local Development Corporation

Defense and Indemnification Policy

Each board member of the corporation shall be provided a defense and be indemnified by the corporation against any and all claims and liabilities to which he or she has or shall become subject by reason of serving or having served as director, or by reason of any action alleged to have been taken, omitted, or neglected by him or her as director; and the corporation shall reimburse each such person for all legal expenses reasonably incurred by him or her in connection with any such claim or liability, provided, however, that no such person shall be indemnified against, or be reimbursed for any expense incurred in connection with , any clam of liability arising out of his or her own willful misconduct or gross negligence.

The amount paid to any director by way of indemnification shall not exceed his or her actual, reasonable, and necessary expenses incurred in connection with the matter involved.

The right of indemnification provided for above shall not be exclusive of any rights to which any director of the corporation may otherwise be entitled by law.

Tioga County Local Development Corporation
Code of Ethics

This Code of Ethics shall apply to all officers and employees of the Tioga County Local Development Corporation. These policies shall serve as a guide for official conduct and are intended to enhance the ethical and professional performance of the Corporation's directors and employees and to preserve public confidence in the Corporation's mission.

Responsibility of Directors and Employees

1. Directors and employees shall perform their duties with transparency, without favor and refrain from engaging in outside matters of financial or personal interest, including other employment, that could impair independence of judgment, or prevent the proper exercise of one's official duties.

2. Directors and employees shall not directly or indirectly, make, advise, or assist any person to make any financial investment based upon information available through the director's or employee's official position that could create any conflict between their public duties and interests and their private interests.

3. Directors and employees shall not solicit, directly or indirectly, any gifts or receive or accept any gift having the value of Seventy-five ($75.00) Dollars, or more, whether in the form of money, services, loan, travel, entertainment, hospitality, thing or promise, or in any other form, under circumstances in which it could be reasonably inferred that the gift was intended to influence him or her, or could reasonably be expected to influence him or her in the performance of his or her official duties or was intended as a reward for any official action on his or her part.

4. Directors and employees shall not use or attempt to use their official position with the Corporation to secure unwarranted privileges for themselves, members of their family or others, including employment with the Corporation or contracts for materials or services with the Corporation.

5. Directors and employees must conduct themselves at all times in a manner that avoids any appearance that they can be improperly or unduly influenced, that they could be affected by the position of or relationship with any other party, or that they are acting in violation of their public trust.

6. Directors and employees may not engage in any official transaction with an outside entity in which they have a direct or indirect financial interest that may reasonably conflict with the proper discharge of their official duties.

7. Directors and employees shall manage all matters within the scope of the Corporation's mission independent of any other affiliations or employment. Directors, including ex officio board members, and employees employed by more than one government shall strive to fulfill their professional responsibility to the Corporation without bias and shall support the Corporation's mission to the fullest.

8. Directors and employees shall not use Corporation property, including equipment, telephones, vehicles, computers, or other resources, or disclose information acquired in the course of their official duties in a manner inconsistent with State or local law or policy and the Corporation's mission and goals.

Implementation of Code of Ethics

This Code of Ethics shall be provided to all directors and employees upon commencement of employment or appointment and shall be reviewed annually by the Governance Committee.

The board may designate an Ethics Officer, who shall report to the board and shall have the following duties:

- Counsel in confidence Corporation directors and employees who seek advice about ethical behavior.
- Receive and investigate complaints about possible ethics violations.
- Dismiss complaints found to be without substance.
- Prepare an investigative report of their findings for action by the President of the board.
- Record the receipt of gifts or gratuities of any kind received by a director or employee, who shall notify the Ethics Officer within 48 hours of receipt of such gifts and gratuities.

Penalties

In addition to any penalty contained in any other provision of law, a Corporation director or employee who knowingly and intentionally violates any of the provisions of this code may be removed in the manner provided for in law, rules or regulations.

Reporting Unethical Behavior

Employees and directors are required to report possible unethical behavior by any director or employee of the Corporation to the Ethics Officer. Employees and directors may file ethics complaints anonymously and are protected from retaliation by the policies adopted by the Corporation.

Tioga County Local Development Corporation
Use of Discretionary Funds

Provisions: Section 2824(1)(b) of Public Authorities Law requires directors to understand, review and monitor the implementation of fundamental financial and management controls and the operating decisions of the authority.

Objectives: Boards of directors and authority management have an obligation to authorize the expenditure of funds only for purposes that relate to and support the mission of the authority. The fiduciary duty of the board includes adopting policies that safeguard the assets and resources of the authority and protect against the use of funds for purposes that do not advance its core purpose and objectives.

Recommended Practice: The Office of the Attorney General determined that the expenditure of authority funds must relate directly to an enumerated power, duty or purpose of the authority. The funds of an authority may not be spent in support of the private or personal interests or to the benefit of directors, management or staff. This policy addresses not only what constitutes a proper discretionary expenditure related to the mission and public purpose of the authority, but also addresses what would be considered an improper use of those funds.

Proper Use:

- Certain out-of-town business travel and travel-related expenses are appropriate to advance the mission of the authority. A reasonable amount for such expense shall be exercised and employees shall perform due diligence to obtain the lowest cost. Prior approval or authorization by the director will ensure that such travel is reasonable and necessary. Documentation to justify the nature and purpose of travel expenses is required and the employee shall provide receipts for expenses. (Amounts used are typically allowed by federal GSA guidelines for travel expenses including per diems, government lodging rates and amounts for meals and other incidental expenses).

- Certain meal costs also may be incurred through participation in, or sponsorship of, activities integral to meeting the core public purpose of the authority. Similar to appropriate travel expenses, eligible meal costs must be properly documented and reasonable cost thresholds established.

Improper Use:

- Purchases using authority cash or credit that are personal in nature, that would benefit one or more staff of the authority rather than benefit those dependent on the authority's services, or are not necessary to advance the mission of the authority are not allowed. Examples of inappropriate use of authority funds would include, but need not be limited to:

  • Food, beverages, and other refreshments purchased for the personal use of directors, management or other employees or by persons with whom the authority conducts business (unless prior authorization is received);

  • Flowers and gifts for staff, directors or family members;

  • Subsidized or free use of authority services for the personal use of current or former board members, staff, or family members of staff;

  • Celebrations for special occasions that do not directly relate to the purpose of the authority, such as catering or decorations for summer picnics, office parties or holiday or retirement parties;

  • Charitable contributions or sponsorships of events not associated with the authority's mission;

  • Purchases of tobacco products;

  • Membership dues in professional organizations on behalf of employees;

  • Renewal of professional licenses for staff;

  • Personal use of authority vehicles, unless properly documented for tax purposes;

  • Costs to purchase or mail holiday cards, invitations or expressions of sympathy to staff or families of authority staff; or

  • Assignment of cell phones or vehicles to non-authority staff.

- Public authorities may not use public funds to purchase items considered personal expenses or that are intended to personally benefit an employee or director. Expenses such as those listed above do not advance a public purpose and should be considered personal in nature.

MINORITY & WOMEN'S BUSINESS ENTERPRISE POLICY

It is the policy of the Local Development Corporation to take affirmative action to ensure that minority business enterprises (MBEs), i.e., independent business concerns which are at least 51 percent owned and controlled by minority group members (citizens of the United States or permanent resident aliens who are Black, Hispanic, Asian, or American Indian), and women-owned business enterprises (WBEs), i.e., independent business concerns which are at least 51 percent owned and controlled by a women who are citizens of the United States or permanent resident aliens, are given the opportunity to demonstrate their ability to provide the LDC with goods and services at competitive prices.

Company Credit Cards

The Company shall issue a company credit card where the nature of an employee's job requires such use. Company credit cards may only be used for business expenses and may not be used for expenses of a personal nature. Credit cards are issued at the discretion of the President.

The purpose of this Statement of Policy and Procedure is to ensure that company credit cards are used for appropriate purposes and that adequate controls are established for day-to-day use. The Company Credit Cards policy applies to all employees who maintain a credit card for company use.

The President shall maintain rules and regulations and procedures governing the use of the issued cards. Individuals who are issued cards shall annually sign an agreement regarding use of the credit card. In the case of the President, such approvals shall be received through a member of the Executive Committee, or such member as may be designated by the Board of Directors.

The Company reserves the right to withdraw any company issued credit card immediately and without cause.

RESPONSIBILITY

Individuals holding Company Credit Cards are responsible for:

- Using the cards only for their intended purpose
- Retaining receipts and providing explanations for all company credit card transactions
- Obtaining authorization for credit card invoices

The President or her designee is responsible for:

- Limiting the use of company credit cards to those employees who require a card for company business; identifying and requesting any credit or transaction-level limits required for individual cards
- Reviewing and authorizing credit card invoices used by employees on a timely basis to avoid late payment charges; ensuring that all credit card transactions are properly authorized
- Processing payments for credit card invoices on a timely basis to avoid late payment charges

Date: April 3, 2014 TCLDC
Reviewed: 3/3/2015

SECTION 1: PURPOSE AND AUTHORITY

The purpose of this document is to outline the procurement policy (the "Policy") of the Tioga County Local Development Corporation (the "Corporation") applicable to procurement of goods and services paid for by the Corporation for its own use and benefit. The Act requires that goods and services must be procured by the Corporation in such a manner so as to assure the prudent and economic use of public funds, to facilitate the acquisition of goods and services of maximum quality at the lowest possible cost under the circumstances, and to guard against favoritism, improvidence, extravagance, fraud and corruption.

SECTION 2: SECURING GOODS AND SERVICES

Each action taken in connection with each procurement must be supported by documentation. When an award is made to other than the lowest responsible offeror, the determination to make the award must be supported by documentation that justifies the award and sets forth the reasons why the award furthers the purposes of this Policy and provisions of section 104-b of the New York General Municipal Law.

SECTION 3: METHOD OF PURCHASE

The following method of Purchase will be used when required by this Policy in order to achieve the highest quality and savings:

Estimated Amount of Purchase	Method Required
Up to $500	Discretion of the President or Designee employing reasonable methods to secure best pricing available under prevailing circumstances
$501 - $4,999	3 verbal quotations employing reasonable methods to secure best pricing available under prevailing circumstances with written documentation of conversation to file
$5,000 to $9,999	lowest responsible bidder price based on 3 written/fax quotations in response to a request for proposal unless emergency circumstances dictate otherwise, in which case such circumstances shall be documented in writing
$10,000 and above	Lowest responsible bidder in response to advertisement for sealed bids pursuant to section 103 of the General Municipal Law, except as otherwise permitted by Article 5-A of the General Municipal Law

Number of Proposals or Quotations

A good faith effort shall be made to obtain the required number of proposals or quotations. If the purchaser is unable to obtain the required number of proposals or quotations, the purchaser will document the attempt made at obtaining the proposals. In no event shall the failure to obtain the proposals be a bar to the procurement.

Documentation

Documentation is required for each action taken in connection with each procurement. Documentation and an explanation are required whenever a contract is awarded to other than the lowest responsible bidder. This documentation will include an explanation of how the award will achieve savings or how the bidder was not acceptable. A determination that the bidder is not acceptable shall be made by the purchaser with the approval of the Audit Committee.

SECTION 4: CIRCUMSTANCES WHERE SOLICITATION OF ALTERNATIVE PROPOSALS AND QUOTATIONS ARE NOT IN THE BEST INTEREST OF THE CORPORATION

Pursuant to Section 104-b (2) (f) of the General Municipal Law, this policy may contain circumstances when, or types of procurement for which, in the sole discretion of the members of the Corporation, the solicitation of alternative proposals or quotations will not be in the best interest of the Corporation. In the following circumstances, it may not be in the best interest of the Corporation to solicit quotations or document the basis for not accepting the lowest bid.

Professional and Contracted Services

Professional services or services requiring special or technical skill, training or expertise. The individual, company or firm must be chosen based on accountability, reliability, responsibility, skill, conflict of interests, reputation, education and training, judgment, integrity, continuity of service and moral worth. Furthermore, certain professional services to be provided to the Corporation, e.g., legal and accounting services, impact liability issues of the Corporation and its members, including securities liability in circumstances where the Corporation is issuing bonds. These qualifications and the concerns of the Corporation regarding its liability and the liability of its members are not necessarily found or addressed in the individual, company or firm that offers the lowest price and the nature of these services are such that they do not readily lend themselves to competitive procurement procedures.

In determining whether a service fits into this category, the Corporation shall take into consideration the following guidelines: (a) whether the services are subject to state licensing or testing requirements; (b) whether substantial formal education or training and experience is a necessary prerequisite to performance of the services. Professional or technical services shall include but not be limited to the following: services of an attorney (including bond counsel); services of a physician; technical services of an engineer engaged to prepare plans, maps and estimates; securing insurance coverage and/or services of an insurance broker; services of a certified public accountant; investment management services; marketing, advertising and/or printing services involving extensive writing, editing, or art work; management of Corporation-owned property; and computer software or programming services for customized programs, or services involved in substantial modification and customizing of pre-package software.

Emergency Purchases

Emergency purchases pursuant to Section 103(4) of the General Municipal Law. Due to the nature of this exception, these goods or services must be purchased immediately and a delay in order to seek alternate proposals may threaten the life, health, safety or welfare of the public. This section does not preclude alternate proposals if time permits. The President or

Designee shall obtain a verbal quote, at a minimum, which shall be documented and shall also include a description of the facts giving rise to the emergency and that it meets the criteria set forth herein. Said documentation may also include the opinions of Counsel regarding the exception from bidding.

Purchases of Secondhand Goods

If alternate proposals are required, the Corporation is precluded from purchasing surplus and second-hand goods at auctions or through specific advertising sources where the best prices are usually obtained. It is also difficult to try to compare prices of used goods and a lower price may indicate an older product.

Sole Source

Defined as a situation when there is only one possible source item which to procure goods and/or services and it is shown that the item needed has unique a benefit, the cost is reasonable for the product offered and there is not competition available. In this situation, a request for a resolution waiving bidding requirements is required.

Goods or Services Under $500

The time and documentation required to Purchase through this Policy may be more costly than the item itself and would therefore not be in the best interest of the taxpayer. In addition, it is not likely that such minimal contracts would be awarded based on favoritism.

Buy Local

Reasonable preference will be given to making purchases from Tioga County businesses.

SECTION 5: UNINTENTIONAL FAILURE TO COMPLY

The unintentional failure to comply with the provision of Section 104-b of the General Municipal Law shall not be grounds to void action taken or give rise to a cause of action against the Corporation or any officer thereof.

SECTION 6: POLICY REVIEW

The statute requires that the Policy must be reviewed by the Corporation annually. Any amendments will be approved by the Corporation's Board of Directors.

Tioga County Local Development Corporation

Property Disposition Policy

In keeping with the policy of maintaining the highest standards of conduct and ethics and to operate in the most accountable and open manner, the Tioga County Local Development Corporation (the "Corporation") will maintain adequate inventory controls and accountability systems for all Property (as such term is defined below) under its control. Furthermore, the Corporation will dispose (as such term is defined below) of Property in compliance with any applicable Law, Rule or Regulation (as such term is defined below). Failure to follow the provisions of this Property Disposition Policy will result in disciplinary action including possible termination of employment, dismissal from one's board or agent duties and possible civil or criminal prosecution if warranted.

Definitions

Contracting Officer shall mean the Executive Director of the Corporation.

Dispose, Disposed or Disposal shall mean the transfer of title or any other beneficial interest in personal or real property in accordance with Section 2897 of the New York Public Authorities Law.

Law, Rule or Regulation: Any duly enacted statute, or ordinance or any rule or regulation promulgated pursuant to any federal, state or local statute or ordinance.

Property shall mean (a) personal property in excess of five thousand dollars ($5,000.00) in value, (b) real property, and (c) any inchoate or other interest in such property, to the extent that such interest may be conveyed to another person for any purpose, excluding an interest securing a loan or other financial obligation of another party.

Operative Policy

Inventory Controls and Accountability Systems

The Contracting Officer of the Corporation shall be responsible for the Corporation's compliance with this Property Disposition Policy and will act under the direction of the Board of Directors regarding the supervision and control of all Property Disposed of by the Corporation. In addition, the Contracting Officer shall have the responsibility to insure the Corporation operates in compliance with Title 5-A of the New York Public Authorities Law, including creating and maintaining adequate inventory controls and accountability systems for all property under the control of the Corporation and periodically inventorying such property to recommend which, if any, property should be Disposed by the Corporation.

Disposition of Property

Unless otherwise authorized by this Policy, the Corporation shall Dispose of Property for not less than fair market value ("FMV") by sale, exchange, or transfer, for cash, credit, or other property, with or without warranty, and upon such terms and conditions as the board deems proper. Provided, however, that no disposition of real property, any interest in real property, or any other Property which because of its unique nature is not subject to fair market pricing shall be made unless an appraisal of the value of such Property has been made by an independent appraiser and included in the record of the transaction.

Unless otherwise authorized by this Policy, prior to disposing of Property or entering into a contract for the Disposal of Property, the Corporation shall publicly advertise for bids for such Disposal or contract for Disposal. The advertisement for bids shall be made at such a time prior to the Disposal or contract for Disposal, through such methods, and on such terms and conditions as shall permit full and free competition consistent with the value and nature of the Property. Such advertisement shall include the date, time and place the bids will be publicly disclosed by the Corporation. The Corporation shall award the contract with reasonable promptness to the most reasonable bidder whose bid, conforming to the invitation for bids, is most advantageous to the Tioga County Local Development Corporation (the "Corporation"), price and other factors considered; provided, however, that the Corporation reserves the right to reject all such bids when it is in the public interest to do so.

The Corporation may Dispose of Property or enter into contracts for the disposal of Property via negotiation or public auction without regard to the two (2) paragraphs immediately above, but subject to obtaining such competition as is feasible under the circumstances, if:

(i) the personal property involved is of a nature and quantity which, if Disposed under the first two (2) paragraphs of this section, would adversely affect the state of local market for such Property, and the estimated FMV of such Property and other satisfactory terms of the Disposal can be obtained by negation;

(ii) the FMV of the Property does not exceed fifteen thousand dollars ($15,000.00)

(iii) bid prices after advertising therefore are not reasonable, either as to all or some part of the Property, or have not been independently arrived at in open competition;

(iv) the Disposal is to the State or any political subdivision of the State, and the estimated FMV of the Property and other satisfactory terms of the Disposal are obtained by negations;

(v) the Disposal is for an amount less than the estimated FMV of the Property, the terms of such Disposal are obtained by public auction or negotiation, the Disposal of the Property is intended to further the public health, safety or welfare or an economic development interest of the State or a political subdivision of the State, including but not limited to, the prevention or remediation of a substantial threat to public health or safety, or the creation or retention of a substantial number of job opportunities, or the creation or retention of a substantial source of revenues, and the purpose and terms of the Disposal are documented in writing and approved by resolution of the Board, or

(vi) such Disposal or related action is otherwise authorized by law.

The Corporation shall file an explanatory statement with the comptroller, the director of the division of budget, the commissioner of general services and the legislature not less than ninety (90) days before the Corporation Disposes the Property if the Property is personal property in excess of fifteen thousand dollars ($15,000.00) or real property that has a fair market value in excess of one hundred thousand dollars ($100,000.00). When the Property is Disposed by lease (or exchange), then the Corporation shall file an explanatory statement when the Property is real property leased for a term of five (5) years or less with and estimated fair annual rent exceeding one hundred thousand dollars ($100,000.00) in any given year, real property leased for a term greater than five (5) years with an estimated fair annual rent exceeding one hundred thousand dollars ($100,000.00) for the entire lease term; or any real property or real and related personal property Disposed of by exchange, regardless of value, or any property any part of the consideration for which is real property.

Reporting Requirements

Annual Report

The Corporation shall publish, at least annually, an Annual Report (the "Annual Report") listing all Property consisting of real property of the Corporation. In addition, the Annual Report shall include a list and full description of all Property consisting of real and personal property disposed of during such period covered by the Annual Report. The Annual Report shall include the price received by the Corporation for the Property, in addition to the name of the purchase for all such Property sold by the Corporation during such period covered by the Annual Report.

The Corporation shall file copies of the Annual Report with the Office of the State Comptroller and the Authority Budget Office and to the extent practicable, post such Annual Report on its website.

Property Disposition Policy

The Corporation shall review and approve this Property Disposition Policy annually by resolution of the Board. On or before March 31 of each year, the Corporation shall file with the Comptroller a copy of its Property Disposition Policy, including the name of the Contracting Officer appointed by the Corporation. Upon such filing with the comptroller, the Corporation shall post its Property Disposition Policy on its website.

Contracting Officer
Rebecca Maffei

Executive Director
80 North Avenue
Owego New York, 13827
Phone (607) 687-7440
Fax (607) 687-9820

In keeping with the policy of maintaining the highest standards of conduct and ethics, the Tioga County Local Development Corporation (the "Corporation") will investigate any suspected Fraudulent or Dishonest Conduct by an employee, board member or agent of the Corporation. The Corporation is committed to maintaining the highest standards of conduct and ethical behavior and promotes a working environment that values respect, fairness and integrity. All employees, board members and agents shall act with honesty, integrity and openness in all their dealings as representatives for the organization. Failure to follow these standards will result in disciplinary action including possible termination of employment, dismissal from one's board or agent duties and possible civil or criminal prosecution if warranted.

Employees, board members, consultants and agents are encouraged to report suspected acts of Fraudulent or Dishonest Conduct by an employee, board member or agent of the Corporation, (i.e. to act as "Whistle-Blower"), pursuant to the procedures set forth below.

Reporting

A person's concerns about suspected acts of Fraudulent or Dishonest Conduct by an employee, board member or agent of the Corporation should be reported to the President of the Corporation. If for any reason a person finds it difficult to report his or her concerns to the President, the person may report the concerns directly to any other board member. Alternately, to facilitate reporting of suspected violations where the reporter wishes to remain anonymous, a written statement may be submitted to any one of the individuals listed above.

The Governance Committee will then review all claims of Fraudulent or Dishonest Conduct. The Governance Committee will make a recommendation to the full Board with regard to the appropriate action on such claims. Any action taken with regard to the suspected violation will be made by the full Board upon review and discussion of the information gathered by the Governance Committee.

Definitions

Baseless Allegations: Allegations made with reckless disregard for their truth or falsity. People making such allegations may be subject to disciplinary action by the Corporation, and/or legal claims by individuals accused of such conduct.

Fraudulent or Dishonest Conduct: The act of wrongdoing, misconduct, malfeasance or other inappropriate behavior by an employee, board member or agent of the Corporation, including a deliberate act of failure to act with the intention of obtaining an unauthorized benefit. Examples of such conduct include, but are not limited to:

- Forgery or alteration of documents;
- Unauthorized alteration or manipulation of computer files;
- Fraudulent financial reporting;
- Pursuit of a benefit or advantage in violation of the Corporation's Conflict of Interest Policy;
- Misappropriation or misuse of the Corporation's resources, such as funds, supplies or other assets;
- Authorizing or receiving compensation for goods not received or services not performed;
- Authorizing or receiving compensation for hours not worked; and
- The violation of any Law, Rule or Regulation.

Law, Rule or Regulation: Any duly enacted statute, or ordinance or any rule or regulation promulgated pursuant to any federal, state or local statute or ordinance.

Public Body: includes the following:

- The United States Congress, any state legislature, or any popularly-elected local governmental body, or any member or employee thereof;
- Any federal, state or local judiciary, or any member or employee thereof, or any grand or petit jury; and
- Any federal, state, or local law enforcement agency, prosecutorial office, or police or peace office.

Retaliatory Personnel Action: The discharge, suspension or demotion of an employee, or other adverse employment action taken against the employee in terms and conditions of employment, including but not limited to, threats of physical harm, loss of job, punitive work assignments, or impact on salary or fees.

Whistle-Blower: An employee, consultant or agent who informs the President, any board member or Public Body pursuant to the provisions of this policy about an activity relating to the Corporation which that person believes to be Fraudulent or Dishonest Conduct.

Rights and Responsibilities

Supervisors

The Executive Director is required to report suspected Fraudulent or Dishonest Conduct to the President of the Board.

Reasonable care should be taken in dealing with suspected Fraudulent or Dishonest Conduct to avoid:

- Baseless Allegations;
- Premature notice to persons suspected of Fraudulent or Dishonest Conduct and/or disclosure of suspected Fraudulent or Dishonest Conduct to others not involved with the investigation; and
- Violations of a person's rights under law.

Due to the important yet sensitive nature of the suspected Fraudulent or Dishonest Conduct, effective professional follow-up is critical. The President, while appropriately concerned about properly examining such issues, should not in any circumstances perform any investigative or other follow up steps on his own. Accordingly, when the President becomes aware of suspected Fraudulent or Dishonest Conduct he:

- Should contact the full Board of Directors and inform all of the suspected Fraudulent or Dishonest Conduct and inform the Board that the Governance Committee will be gathering information related to the claim;
- Should not contact the person suspected of Fraudulent or Dishonest Conduct to further investigate the matter or demand restitution;
- Should not discuss the case with attorneys other than counsel to the Corporation, the media or anyone other than the members of the Board; and

- Should not report the case to an authorized law enforcement officer without first discussing the case with the members of the Board.

Investigation

All relevant matters, including suspected but unproved allegations of Fraudulent or Dishonest Conduct, will be reviewed and analyzed, with documentation of the receipt, retention, investigation and treatment of the complaint by the Governance Committee. Upon full Board review of the Committee report, appropriate corrective action will be taken, if necessary, and findings will be communicated back to the reporting person, if appropriate. Investigations may warrant investigation by an independent person such as auditors and/or attorneys if so determined by the full Board of Directors.

Whistle-Blower Protection

The Corporation will protect a Whistle-Blower pursuant to the guidelines set forth below.

- The Corporation will use its best efforts to protect a Whistle-Blower against all Retaliatory Personnel Actions. Whistle-Blowing complaints will be handled with sensitivity and discretion to the extent allowed by the circumstances and law. Generally, this means that Whistle-Blower complaints will only be shared with those who have a need to know including, if appropriate, law enforcement personnel, so that the Corporation can conduct an effective investigation and determine what action is required based on the results of any such investigation. (Should disciplinary or legal action be taken against a person or persons as a result of a Whistle-Blower complaint, such persons may also have the right to know the identity of the Whistle-Blower.);

- Employees, board members, consultants and agents of the Corporation may not engage in any Retaliatory Personnel Action against a Whistle-Blower for (i) disclosing or threatening to disclose to the President or a board member, as applicable, any activity which that person believes to be Fraudulent or Dishonest Conduct, or (ii) objecting to or refusing to participate in any Fraudulent or Dishonest Conduct. A Whistle-Blower who believes that he has been the victim of a Retaliatory Personnel Action may file a written complaint with the President or any board member, as applicable. Any complaint of a Retaliatory Personnel Action will be promptly investigated by the Governance Committee and appropriate corrective measures, as determined by the full Board of Directors, will be taken if such allegations are substantiated. This protection from Retaliatory Personnel Action is not intended to prohibit supervisors from taking action, including disciplinary action, in the usual scope of their duties and based on valid performance-related factors;

- Employees, board members, consultants and agents of the Corporation may not engage in any Retaliatory Personnel Action against a Whistle-Blower for (i) disclosing, or threatening to disclose to a Public Body any activity which that person believes to be Fraudulent or Dishonest Conduct, or (ii) providing information to, or testifying before, any Public Body conducting an investigation, hearing or inquiry into any such Fraudulent or Dishonest Conduct. Provided, however, that a Whistle-Blower who discloses or threatens to disclose any Fraudulent or Dishonest Conduct to a Public Body is not covered under this policy unless he first brings the allegation of Fraudulent or Dishonest Conduct to the attention of the President or any board member, as applicable, and has afforded the Corporation a reasonable opportunity to correct or remedy such Fraudulent or Dishonest Conduct; and

- A Whistle-Blower must be cautious to avoid Baseless Allegations.

Sexual Harassent Policy for All Employers in New York State

Introduction

Tioga County Local Development Corporation (TC LDC) is committed to maintaining a workplace free from sexual harassment. Sexual harassment is a form of workplace discrimination. All employees are required to work in a manner that prevents sexual harassment in the workplace. This Policy is one component of TC LDC commitment to a discrimination-free work environment. Sexual harassment is against the law[1] and all employees have a legal right to a workplace free from sexual harassment and employees are urged to report sexual harassment by filing a complaint internally with TC LDC.
Employees can also file a complaint with a government agency or in court under federal, state or local antidiscrimination laws.

Policy:

1. TC LDC policy applies to all employees, applicants for employment, interns, whether paid or unpaid, contractors and persons conducting business, regardless of immigration status, with TC LDC. In the remainder of this document, the term "employees" refers to this collective group.

2. Sexual harassment will not be tolerated. Any employee or individual covered by this policy who engages in sexual harassment or retaliation will be subject to remedial and/or disciplinary action (e.g., counseling, suspension, termination).

3. Retaliation Prohibition: No person covered by this Policy shall be subject to adverse action because the employee reports an incident of sexual harassment, provides information, or otherwise assists in any investigation of a sexual harassment complaint. TC LDC will not tolerate such retaliation against anyone who, in good faith, reports or provides information about suspected sexual harassment. Any employee of TC LDC who retaliates against anyone involved in a sexual harassment investigation will be subjected to disciplinary action, up to and including termination. All employees, paid or unpaid interns, or non-employees[2] working in the workplace who believe they have been subject to such retaliation should inform a supervisor, manager, or TC LDC Board Chair. All employees, paid or unpaid interns or non-employees who believe they have been a target of such retaliation may also seek relief in other available forums, as explained below in the section on Legal Protections.

[1] While this policy specifically addresses sexual harassment, harassment because of and discrimination against persons of all protected classes is prohibited. In New York State, such classes includeage, race, creed, color, national origin, sexual orientation, military status, sex, disability, marital status, domestic violence victim status, gender identity and criminal history.

[2] A non-employee is someone who is (or is employed by) a contractor, subcontractor, vendor, consultant, or anyone providing services in the workplace. Protected non-employees include persons commonly referred to as independent contractors, "gig" workers and temporary workers. Also included are persons providing equipment repair, cleaning services or any other services provided pursuant to a contract with the employer.

Adoption of this policy does not constitute a conclusive defense to charges of unlawful sexual harassment. Each claim of sexual harassment will be determined in accordance with existing legal standards, with due consideration of the particular facts and circumstances of the claim, including but not limited to the existence of an effective anti-harassment policy and procedure.

4. Sexual harassment is offensive, is a violation of our policies, is unlawful, and may subject TC LDC to liability for harm to targets of sexual harassment. Harassers may also be individually subject to liability. Employees of every level who engage in sexual harassment, including managers and supervisors who engage in sexual harassment or who allow such behavior to continue, will be penalized for such misconduct.

5. TC LDC will conduct a prompt and thorough investigation that ensures due process for all parties, whenever management receives a complaint about sexual harassment, or otherwise knows of possible sexual harassment occurring. TC LDC will keep the investigation confidential to the extent possible. Effective corrective action will be taken whenever sexual harassment is found to have occurred. All employees, including managers and supervisors, are required to cooperate with any internal investigation of sexual harassment.

6. All employees are encouraged to report any harassment or behaviors that violate this policy. TC LDC will provide all employees a complaint form for employees to report harassment and file complaints.

7. Managers and supervisors are **required** to report any complaint that they receive, or any harassment that they observe or become aware of, to TC LDC Board Chair.

8. This policy applies to all employees, paid or unpaid interns, and non-employees and all must follow and uphold this policy. This policy must be provided to all employees and should be posted prominently in all work locations to the extent practicable (for example, in a main office, not an offsite work location) and be provided to employees upon hiring.

What Is "Sexual Harassment"?

Sexual harassment is a form of sex discrimination and is unlawful under federal, state, and (where applicable) local law. Sexual harassment includes harassment on the basis of sex, sexual orientation, self-identified or perceived sex, gender expression, gender identity and the status of being transgender.

Sexual harassment includes unwelcome conduct which is either of a sexual nature, or which is directed at an individual because of that individual's sex when:

- Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive work environment, even if the

reporting individual is not the intended target of the sexual harassment;

- Such conduct is made either explicitly or implicitly a term or condition of employment; or

- Submission to or rejection of such conduct is used as the basis for employment decisions affecting an individual's employment.

A sexually harassing hostile work environment includes, but is not limited to, words, signs, jokes, pranks, intimidation or physical violence which are of a sexual nature, or which are directed at an individual because of that individual's sex. Sexual harassment also consists of any unwanted verbal or physical advances, sexually explicit derogatory statements or sexually discriminatory remarks made by someone which are offensive or objectionable to the recipient, which cause the recipient discomfort or humiliation, which interfere with the recipient's job performance.

Sexual harassment also occurs when a person in authority tries to trade job benefits for sexual favors. This can include hiring, promotion, continued employment or any other terms, conditions or privileges of employment. This is also called "quid pro quo" harassment.

Any employee who feels harassed should report so that any violation of this policy can be corrected promptly. Any harassing conduct, even a single incident, can be addressed under this policy.

Examples of sexual harassment

The following describes some of the types of acts that may be unlawful sexual harassment and that are strictly prohibited:

- Physical acts of a sexual nature, such as:
    - Touching, pinching, patting, kissing, hugging, grabbing, brushing against another employee's body or poking another employee's body;
    - Rape, sexual battery, molestation or attempts to commit these assaults.

- Unwanted sexual advances or propositions, such as:
    - Requests for sexual favors accompanied by implied or overt threats concerning the target's job performance evaluation, a promotion or other job benefits or detriments;
    - Subtle or obvious pressure for unwelcome sexual activities.

- Sexually oriented gestures, noises, remarks or jokes, or comments about a person's sexuality or sexual experience, which create a hostile work environment.

- Sex stereotyping occurs when conduct or personality traits are considered inappropriate simply because they may not conform to other people's ideas or perceptions about how individuals of a particular sex should act or look.

- Sexual or discriminatory displays or publications anywhere in the workplace, such as:
    - Displaying pictures, posters, calendars, graffiti, objects, promotional material, reading materials or other materials that are sexually demeaning or pornographic. This includes such sexual displays on workplace computers or cell phones and sharing such displays while in the workplace.

- Hostile actions taken against an individual because of that individual's sex, sexual orientation, gender identity and the status of being transgender, such as:
    - Interfering with, destroying or damaging a person's workstation, tools or equipment, or otherwise interfering with the individual's ability to perform the job;
    - Sabotaging an individual's work;
    - Bullying, yelling, name-calling.

Who can be a target of sexual harassment?

Sexual harassment can occur between any individuals, regardless of their sex or gender. New York Law protects employees, paid or unpaid interns, and non-employees, including independent contractors, and those employed by companies contracting to provide services in the workplace. Harassers can be a superior, a subordinate, a coworker or anyone in the workplace including an independent contractor, contract worker, vendor, client, customer or visitor.

Where can sexual harassment occur?

Unlawful sexual harassment is not limited to the physical workplace itself. It can occur while employees are traveling for business or at employer sponsored events or parties. Calls, texts, emails, and social media usage by employees can constitute unlawful workplace harassment, even if they occur away from the workplace premises, on personal devices or during non-work hours.

Retaliation

Unlawful retaliation can be any action that could discourage a worker from coming forward to make or support a sexual harassment claim. Adverse action need not be job-related or occur in the workplace to constitute unlawful retaliation (e.g., threats of physical violence outside of work hours).

Such retaliation is unlawful under federal, state, and (where applicable) local law. The New York State Human Rights Law protects any individual who has engaged in "protected activity." Protected activity occurs when a person has:

- made a complaint of sexual harassment, either internally or with any anti-discrimination agency;
- testified or assisted in a proceeding involving sexual harassment under the Human Rights Law or other anti-discrimination law;
- opposed sexual harassment by making a verbal or informal complaint to management, or by simply informing a supervisor or manager of harassment;
- reported that another employee has been sexually harassed; or
- encouraged a fellow employee to report harassment.

Even if the alleged harassment does not turn out to rise to the level of a violation of law, the individual is protected from retaliation if the person had a good faith belief that the practices were unlawful.

However, the retaliation provision is not intended to protect persons making intentionally false charges of harassment.

Reporting Sexual Harassment

Preventing sexual harassment is everyone's responsibility. TC LDC cannot prevent or remedy sexual harassment unless it knows about it. Any employee, paid or unpaid intern or non- employee who has been subjected to behavior that may constitute sexual harassment is encouraged to report such behavior to a supervisor, manager or TC LDC Board Chair. Anyone who witnesses or becomes aware of potential instances of sexual harassment should report such behavior to a supervisor, manager or TC LDC Board Chair.

Reports of sexual harassment may be made verbally or in writing. A form for submission of a written complaint is attached to this Policy, and all employees are encouraged to use this complaint form. Employees who are reporting sexual harassment on behalf of other employees should use the complaint form and note that it is on another employee's behalf.

Employees, paid or unpaid interns or non-employees who believe they have been a target of sexual harassment may also seek assistance in other available forums, as explained below in the section on Legal Protections.

Supervisory Responsibilities

All supervisors and managers who receive a complaint or information about suspected sexual harassment, observe what may be sexually harassing behavior or for any reason suspect that sexual harassment is occurring, **are required** to report such suspected sexual harassment to TC LDC Board Chair.

In addition to being subject to discipline if they engaged in sexually harassing conduct themselves, supervisors and managers will be subject to discipline for failing to report suspected sexual harassment or otherwise knowingly allowing sexual harassment to continue.

Supervisors and managers will also be subject to discipline for engaging in any retaliation.

Complaint and Investigation of Sexual Harassment

All complaints or information about sexual harassment will be investigated, whether that information was reported in verbal or written form. Investigations will be conducted in a timely manner, and will be confidential to the extent possible.

An investigation of any complaint, information or knowledge of suspected sexual harassment will be prompt and thorough, commenced immediately and completed as soon as possible. The investigation will be kept confidential to the extent possible. All persons involved, including complainants, witnesses and alleged harassers will be accorded due process, as outlined below, to protect their rights to a fair and impartial investigation.

Any employee may be required to cooperate as needed in an investigation of suspected sexual harassment. TC LDC will not tolerate retaliation against employees who file complaints, support another's complaint or participate in an investigation regarding a violation of this policy.

While the process may vary from case to case, investigations should be done in accordance with the following steps:

- Upon receipt of complaint, TC LDC Board Chair will conduct an immediate review of the allegations, and take any interim actions (e.g., instructing the respondent to refrain from communications with the complainant), as appropriate. If complaint is verbal, encourage the individual to complete the "Complaint Form" in writing. If he or she refuses, prepare a Complaint Form based on the verbal reporting.

- If documents, emails or phone records are relevant to the investigation, take steps to obtain and preserve them.

- Request and review all relevant documents, including all electronic communications.

- Interview all parties involved, including any relevant witnesses;

- Create a written documentation of the investigation (such as a letter, memo or email), which contains the following:
    - A list of all documents reviewed, along with a detailed summary of relevant documents;
    - A list of names of those interviewed, along with a detailed summary of their statements;
    - A timeline of events;
    - A summary of prior relevant incidents, reported or unreported; and
    - The basis for the decision and final resolution of the complaint, together with any corrective action(s).

- Keep the written documentation and associated documents in a secure and confidential location.

- Promptly notify the individual who reported and the individual(s) about whom the complaint was made of the final determination and implement any corrective actions identified in the written document.

- Inform the individual who reported of the right to file a complaint or charge externally as outlined in the next section.

Legal Protections And External Remedies

Sexual harassment is not only prohibited by TC LDC but is also prohibited by state, federal, and, where applicable, local law.

Aside from the internal process at TC LDC, employees may also choose to pursue legal remedies with the following governmental entities. While a private attorney is not required to file a complaint with a governmental agency, you may seek the legal advice of an attorney.

In addition to those outlined below, employees in certain industries may have additional legal protections.

State Human Rights Law (HRL)

The Human Rights Law (HRL), codified as N.Y. Executive Law, art. 15, § 290 et seq., applies to all employers in New York State with regard to sexual harassment, and protects employees, paid or unpaid interns and non-employees, regardless of immigration status. A complaint alleging violation of the Human Rights Law may be filed either with the Division of Human Rights (DHR) or in New York State Supreme Court.

Complaints with DHR may be filed any time **within one year** of the harassment. If an individual did not file at DHR, they can sue directly in state court under the HRL, **within three years** of the alleged sexual harassment. An individual may not file with DHR if they have already filed a HRL complaint in state court.

Complaining internally to TC LDC does not extend your time to file with DHR or in court. The one year or three years is counted from date of the most recent incident of harassment.

You do not need an attorney to file a complaint with DHR, and there is no cost to file with DHR.

DHR will investigate your complaint and determine whether there is probable cause to believe that sexual harassment has occurred. Probable cause cases are forwarded to a public hearing before an administrative law judge. If sexual harassment is found after a hearing, DHR has the power to award relief, which varies but may include requiring your employer to take action to stop the harassment, or redress the damage caused, including paying of monetary damages, attorney's fees and civil fines.

DHR's main office contact information is: NYS Division of Human Rights, One Fordham Plaza, Fourth Floor, Bronx, New York 10458. You may call (718) 741-8400 or visit: www.dhr.ny.gov.

Contact DHR at (888) 392-3644 or visit dhr.ny.gov/complaint for more information about filing a complaint. The website has a complaint form that can be downloaded, filled out, notarized and mailed to DHR. The website also contains contact information for DHR's regional offices across New York State.

Civil Rights Act of 1964

The United States Equal Employment Opportunity Commission (EEOC) enforces federal anti- discrimination laws, including Title VII of the 1964 federal Civil Rights Act (codified as 42 U.S.C. § 2000e et seq.). An individual can file a complaint with the EEOC anytime within 300 days from the harassment. There is no cost to file a complaint with the EEOC. The EEOC will investigate the complaint, and determine whether there is reasonable cause to believe that discrimination has occurred, at which point the EEOC will issue a Right to Sue letter permitting the individual to file a complaint in federal court.

The EEOC does not hold hearings or award relief, but may take other action including pursuing cases in federal court on behalf of complaining parties. Federal courts may award remedies if discrimination is found to have occurred. In general, private employers must have at least 15 employees to come within the jurisdiction of the EEOC.

An employee alleging discrimination at work can file a “Charge of Discrimination.” The EEOC has district, area, and field offices where complaints can be filed. Contact the EEOC by calling 1-800-669- 4000 (TTY: 1-800-669-6820), visiting their website at www.eeoc.gov or via email at info@eeoc.gov.

If an individual filed an administrative complaint with DHR, DHR will file the complaint with the EEOC to preserve the right to proceed in federal court.

Local Protections

Many localities enforce laws protecting individuals from sexual harassment and discrimination. An individual should contact the county, city or town in which they live to find out if such a law exists. For example, employees who work in New York City may file complaints of sexual harassment with the New York City Commission on Human Rights. Contact their main office at Law Enforcement Bureau of the NYC Commission on Human Rights, 40 Rector Street, 10th Floor, New York, New York; call 311 or (212) 306-7450; or visit www.nyc.gov/html/cchr/html/home/home.shtml.

Contact the Local Police Department

If the harassment involves unwanted physical touching, coerced physical confinement or coerced sex acts, the conduct may constitute a crime. Contact the local police department.

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.

- **Information Security Officer**
  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 Information Security Officer and the County Attorney immediately for investigation. The County Attorney and Information Security Officer 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 Information Security officer immediately. All Personal approved devices lost or stolen that contain Tioga County data must also be reported to the Department Head or supervisor and Information Security officer 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 user name, 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 Information Security Officer at the time of the reported incident. The Information Security Officer and 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 Information Security Officer 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 Information Security Officer 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 writte 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 ISO. All software with Vendor service agreements, requiring access for support, must also be submitted for review and approval by the CIO or ISO. 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 ISO. 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 ISO 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 and 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 Information Security Officer 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, the Information Security Officer, 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 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 id. 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 Information Security Officer.

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 – Information Security Officer

A. Duties and description of an Information Security Officer

The County shall appoint an Information Security Officer who is responsible for implementing and monitoring a consistent data security program. The Information Security Officer 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 ~~e~~very 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 Information Security Officer 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.