Breach Notification Policy

Objective: To ensure that the Town of Windsor's response to any suspected breach of private and confidential information complies with State and Federal laws and minimizes harm to individuals served or employed by the Town of Windsor.

The Town values the protection of private information of individuals in accordance with applicable law and regulations. Further, the Town is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Town policy.

The Town shall educate all individuals who may come into contact with any of the information described below on the Town policy in order to increase IT security awareness. The Town desires to ensure each individual understands his or her responsibilities regarding any potential issues.

a) "Private information" shall mean "personal information" in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number;

2. Driver's license number or non-driver identification card number; or

3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

"Personal information" shall mean any information concerning a person which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) "Breach of the security of the system," shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the Town. Good faith acquisition of personal information by an employee or agent of the Town for the purposes of the Town is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Determining if a Breach has Occurred

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, the Town may consider the following factors, among others:

a) Indications that the information is in the physical possession or control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
b) Indications that the information has been downloaded or copied; or
c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
d) System failure.

Notification Requirements

For any computerized data owned or licensed by the Town that includes private information, the Town shall disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The Town shall consult with the State Office of Information Technology Services to determine the scope of the breach and restoration measures.

For any computerized data maintained by the Town that includes private information which the Town does not own, the Town shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after the law enforcement agency determines that such notification does not compromise the investigation.

Methods of Notification

The required notice shall be directly provided to the affected persons by one or more of the following methods:

a) Written notice;

b) Telephone Notification, with records of all calls being kept;

Additional Notices: in addition to one of the above forms of notice the Town may, at its discretion, perform the following additional forms of notice:

a) E-Mail notice when the Town has an e-mail address for the subject individuals;

b) Conspicuous posting of the notice on the Town's webpage, or any Town signs; and

c) Notification to local media

Regardless of the method by which notice is provided, the notice shall include contact information for the Town and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

In the event that any New York State residents are to be notified, the Town shall notify the New York State Attorney General (AG), the New York State Department of State, and the New York State Office of Information Technology Services as to the timing, content and distribution of the notices and approximate number of affected persons.

In the event that more than five thousand (5,000) New York State residents are to be notified at one time, the Town shall also notify consumer reporting agencies, as defined pursuant to State Technology Law Section 208, as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents. A list of consumer reporting agencies shall be compiled by the State Attorney General and furnished upon request to Towns required to make a notification in accordance with State Technology Law Section 208(2), regarding notification of breach of security of the system.

Acceptable Use Policy

Policy Statement- The Town of Windsor has adopted the following Town of Windsor Computer, Network Resource and Internet Usage Policy:

This policy shall be reviewed on an annual basis and updated as needed. This policy shall supersede and revoke all previous policies. Town computers, Town network resources, and internet access lines within the Town of Windsor Town Hall and within any other Town buildings are to be used only for official business of the Town. In no event are those computers, network resources or internet access lines to be used for the personal purposes. Prohibited personal purposes shall include, but not be limited to, the following of:

(a) creating, sending or receiving any personal letters, personal messages, personal advertising, communications relating to personal commercial activities, jokes or other personal communications,

(b) playing any card games or other games,

(c) using any streaming video services e.g. Netflix, Hulu, YouTube, etc., unless directly related to Town business.

(d) creating, sending, posting, displaying or receiving any pornographic or obscene pictures, text, graphics, images, or materials,

(e) accessing any web sites that contain sexually explicit images and/or related materials, advocate illegal activity, and/or advocate intolerance of others,

(f) creating, sending, posting, or displaying any sexually explicit images and/or related materials,

(g) advocating or promoting any illegal activity, and/or advocating or promoting intolerance of others.

(h) creating, sending, posting, displaying or receiving any offensive, abusive, slanderous, libelous, defamatory, vulgar, harassing or intimidating messages, text, graphics, images or materials,

(i) creating or sending any viruses, worms, hoaxes or chain letters,

(j) engaging in any unwarranted invasion of the personal privacy of any individual,

(k) engaging in any unauthorized disclosure of sensitive or confidential information, or

(l) violating any licensing or copyright restrictions.

Any misuse of a Town computer, network resource, or internet access line, or non-- compliance with the Town's written computer and internet usage policies, may result in one or more of the following consequences:

1. Temporary loss of privileges and/or deactivation of computer/network access/internet access.

2. Permanent loss of privileges and/or deactivation of computer/network access/internet access.

3. Confiscation of Town laptop computer by the proper Town official.

4. Disciplinary actions (including proceedings for removal from office) by the appropriate Town board or Town officials and/or State boards or State officials.

5. Subpoena of data files and/or the application for and execution of a search warrant.

6. Legal prosecution under applicable United States, New York State, and/or Town of Windsor statutes, local laws, ordinances, codes , rules and/or regulations (hereinafter the "Laws").

7. Possible penalties under applicable Laws, including fines and/or imprisonment

The Town of Windsor owns all network facilities, computer systems and e-mail accounts that are provided to Town employees and officials. The Town reserves the right to monitor and audit all usage of Town-owned technology systems, including but not limited to hard drives, e-mails, computer files, and network traffic. No employee or Town official should have an expectation of privacy with regard to the use of Town-owned technology.

Disaster Recovery Plan

Policy Statement: This policy defines acceptable methods for disaster recovery planning, preparedness, management and mitigation of IT systems and services for the Town of Windsor (hereinafter the "Town").

The disaster recovery standards in this policy provide a systematic approach for safeguarding the vital technology and data managed by the Town. This policy provides a framework for the management, development, and implementation and maintenance of a disaster recovery program for the systems and services managed by the Town.

Implementation: the Town shall establish as follows:

1. Appoint a Disaster Recovery Manager. The Disaster Recovery Manager shall be charged with implementing the Town's Disaster Recovery Plan.

Scenarios: There are two planning scenarios that will enable the Town to effectively prepare for and recover from likely potential threats.

1. The main computer system fails due to a lightning strike, catastrophic equipment failure, etc.
2. The Town Hall is destroyed in a natural disaster. In this scenario the Town will simultaneously be responding to other effects of the incident at the same time they are trying to restore computer operations.

General Requirements: The Town shall:

- Continue the Town's contractual relationship with Broome County.
    - The County's data catalogue is accessible via remote access.
    - The County maintains generators to maintain operations in the event of a power failure.

- Maintain rigorous backup routines that assure the data is available to restore. The backup shall entail secure off-site backup of data for the Town's financial other computer data.
    - Financial data shall be backed up by the third party company the Town contracts with.
    - The Town's computer data shall be backed up at least once a week.
- The Town's Disaster Recovery Manager or 3rd Party Provider shall attempt to restore the backup data, no less frequently than once a month, in order to ensure the validity of the backup data.
- Have redundant computer technician services to assure immediate response.
- The Town shall appoint a Disaster Recovery Manager who shall be responsible for remote restoration of Town computer data, in accordance with the then current Town Disaster Recovery Plan.
- The Town's financial data is maintained by a third party software company. This financial data is remotely accessible in the event of a disaster.
    - The Town's Disaster Recovery Manager shall be responsible with coordinating remote access in the event of a disaster.