CYBER SECURITY CITIZEN NOTIFICATION POLICY

1. **Compliance with state law.**

This policy is consistent with the State Technology Law, § 208. Section 208 requires all local governmental entities to notify an individual 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 this policy.

2. **Definitions**.

As used in this chapter, the following terms shall have the meanings indicated:

COMPROMISE OF PRIVATE INFORMATION. The unauthorized acquisition of unencrypted computerized data with private information.

PRIVATE INFORMATION.
A. 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.

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 of Big Flats. 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 the private information is not used or subject to unauthorized disclosure.

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

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

TOWN. shall mean the Town of Big Flats

CONSUMER REPORTING AGENCY shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies has been compiled by the state attorney general and is available upon request to Towns required to make a notification under subdivision two of this section.

3. **Unencrypted data**.

If encrypted data is compromised along with the corresponding encryption key, the data shall be considered unencrypted and thus fall under the notification requirements.

4. **Notification of compromise of private information**.

If the Town owns or licenses computerized data that includes private information it shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of the State of New York whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, section 5 herein, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

If the Town maintains computerized data that includes private information which it does not own 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 Town, after consulting with the state Office of Cyber security and Critical Infrastructure Coordination to determine the scope of the breach and restoration measures, shall notify an individual when it has been determined that there has been, or is reasonably believed to have been, a compromise of private information through unauthorized disclosure.

5. **Delay of notification possible in criminal investigations**.

Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

6. **Methods for notification**.

The Town will notify the affected individual. Such notice shall be directly provided to the affected persons by one of the following methods:
A. Written notice;

B. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the Town who notifies affected persons in such form; but that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;
C. Telephone notification, provided that a log of each such notification is kept by the Town which notifies affected persons; or
D. Substitute notice, if the Town demonstrates to the State Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 5,000, or the Town does not have sufficient contact information, substitute notice shall consist of all of the following:
(1) E-mail notice when the Town has an e-mail address for the subject persons;
(2) Conspicuous posting of the notice on the Town's web site page, if the Town maintains one; and
(3) Notification to major state-wide media.

7. **Contents of notice**.

Regardless of the method by which notice is provided, such notice shall include contact information for the Town making the notification 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.

8**. Notification to State and consumer reporting agencies**.

In the event that any New York residents are to be notified, the Town shall notify the State Attorney General, the Consumer Protection Board and the State Office of Cyber Security and Critical Infrastructure Coordination 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 residents.

9. **Notification of more than 5,000 residents**.

When more than 5,000 New York residents are to be notified at one time, then the Town shall notify the consumer reporting agencies, as that term is defined in the State Technologies Law, § 208, as to the timing, content and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.