TOWN OF WINDSOR, COUNTY OF BROOME, STATE OF NEW YORK
Approving the Adoption of Breach Notification Policy Resolution #35-2025

PRESENT: **Supervisor Timothy Harting**
Deputy Supervisor Eric Beavers
Council Member Gary M. Hupman
Council Member Mark Odell
Council Member Daniel Colwell

OFFERED BY:
SECONDED BY:

The Town Board (hereinafter "Town Board") of the Town of Windsor (hereinafter "Town"), duly convened in regular session, does hereby resolve as follows:

WHEREAS, the Town of Windsor desires to adopt and implement a Breach Notification Policy (the "Policy"); and

WHEREAS, the purpose of the Policy is to ensure the Town of Windsor complies with State and Federal laws, and minimizes the harm to individuals served or employed by the Town, when responding to a suspected breach of private and confidential information; and

WHEREAS, pursuant to the State Environmental Quality Review Act ("SEQRA"), it has been determined by the Town Board that this constitutes a Type II Action as defined under 6 NYCRR 617.5(20) and (27).

NOW THEREFORE, BE IT RESOLVED that the Town Board of the Town of Windsor, after review and discussion, hereby approves the adoption of the Breach Notification Policy; and it is

FURTHER RESOLVED that the Supervisor is hereby authorized to sign and deliver any documents necessary to effectuate the Policy and implement the same on behalf of the Town; and it is

FURTHER RESOLVED that this resolution shall take effect immediately.

CERTIFICATION

I, Elizabeth Pfister, Clerk of the Town of Windsor, do hereby certify that the foregoing is a true and exact copy of a resolution adopted by the Town Board of the Town of Windsor, Broome County, New York on the 13th day of August, 2025. Said resolution was adopted by the following vote:

Supervisor Timothy Harting:	Voted-
Deputy Supervisor Eric Beavers:	Voted-
Council Member Gary M. Hupman:	Voted-
Council Member Mark Odell:	Voted-
Council Member Daniel Colwell:	Voted-

Motion
Resolution Adopted:

_____
Elizabeth Pfister, Town Clerk
Town of Windsor

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.