Computer System Security Breach Notification Policy
Town of Duanesburg, New York

§ 1-1. Title.

This chapter shall be known as the "Town of Duanesburg Computer System Security Breach Notification Policy."

§ 1-2. Legislative Intent.

This computer system security breach notification policy is intended to establish procedures to follow in the in the event a person(s) has accessed, without valid authorization, private information of individuals from the records of the Town of Duanesburg and to alert said individuals to any potential identity theft as quickly as possible so that they may take appropriate steps to protect themselves from and remedy any impacts of the potential identity theft or security breach.

§1-3. Authority.

This chapter is enacted pursuant to the New York State Constitution, New York Municipal Home Rule Law § 10 and New York State Technology Law § 208.

§1-4. Definitions.

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

BREACH OF SECURITY OF THE SYSTEM — Unauthorized access or access without valid authorization of computerized data which compromises the security, confidentiality or integrity of private information maintained by the Town. Good faith access of private information by an employee or agent of the Town for the purposes of the employee or agent is not used or subject to unauthorized disclosure. In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, the Town may consider the following factors, among others:

A. Indications that the information was viewed, communicated with, used or altered by an unauthorized person; or
B. 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
C. Indications that the information has been downloaded or copied; or
D. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

CONSUMER REPORTING AGENCY — Any person or entity 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 may be obtained upon request of the State Attorney General.

DEPARTMENT — Any board, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the Town.

PERSONAL INFORMATION — Any information concerning a natural person which, because of name, number, personal mark, or other identifier can be used to identify that person.

PRIVATE INFORMATION — Either (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

1. Social security number;
2. Driver's license number or non-driver identification card number;
3. Account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;
4. Account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or
5. Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

TOWN — The Town of Duanesburg, County of Schenectady.

§1-5. Disclosure of Breach to Affected Persons.

A. Any Town department that owns or licenses computerized data that includes private information must disclose any breach of the security of the system to any individual whose private information was, or is reasonably believed to have been, accessed by a person without valid authorization. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in § 1-7 below, or any measures necessary to determine the scope of the breach and restore the integrity of the data system. The Town shall consult with the State Office of Cyber Security and Critical Infrastructure Coordination to determine the scope of the breach and restoration measures.
B. Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private

information, and the Town reasonably determines such exposure will not likely result in misuse of such information, financial harm to the affected persons, or emotional harm in the case of unknown disclosure. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the State Attorney General within ten days of the determination.

C. If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the State Attorney General, the Department of State and the division of State police.

§ 1-6. Disclosure of Breach to Owner or Licensee.

If the Town maintains computerized that data that includes private information which the Town does not own, the Town must 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, accessed by a person without valid authorization.

§ 1-7. Permitted Delay.

Notification pursuant to this policy may be delayed if a law enforcement agency determines that notification could impede a criminal investigation. The notification must be made after the law enforcement agency determines that notification would not compromise any criminal investigation.

§ 1-8. Method of Notification.

The required notice must be directly provided to the affected individuals by one of the following methods:

A. Written notice;
B. Electronic notice, provided that the person to whom the notice is required to be provided has expressly consented to receiving notice in electronic form and a log of each electronic notification is kept by the Town; and provided further that no person or business may require a person to consent to accepting notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;
C. Telephone notification, provided that a log of each telephone notification is kept by the Town; 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 number of individuals to be notified exceeds 500,000, or the Town does not have sufficient contact information. Substitute notice must include 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 website page, if the Town maintains one; and

3. Notification to major state-wide media.

§ 1-9. Information Required.

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

§ 1-10. Notification of Agencies.

A. Whenever any New York State residents are to be notified pursuant to this policy, the Town must 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 the approximate number of affected people. Such notice must be made without delaying notice to affected individuals.
B. Whenever more than 5,000 New York State residents are to be notified at one time, the Town must also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected people. Such notice must be made without delaying notice to affected individuals.

§ 1-11. Severability.

If any clause, sentence, paragraph, subdivision or part of this chapter or the application thereof to any person, firm or corporation, or circumstance, shall be adjudged by any court of competent jurisdiction to be invalid or unconstitutional, such order or judgment shall not affect, impair or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision or part of this chapter or in its application to the person, individual, firm or corporation or circumstance directly involved in the controversy in which such judgment or order shall be rendered.