Village of Ossining- Computer System Security Breach Notification Policy

1. **Title.**

This policy shall be known as the "Village of Ossining Computer System Security Breach Notification Policy."

2. **Purpose.**

This Computer System Security Breach Notification Policy is intended to establish procedures to follow in the event a person(s) has acquired, without valid authorization, private information of individuals from the records of the Village of Ossining 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.

3. **Authority.**

This policy is enacted pursuant to the New York State Technology Law § 208, and may be amended from time to time by Village Board resolution or local law.

4. **Definitions.**

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

BREACH OF SECURITY OF THE SYSTEM

Unauthorized access to or acquisition of, or access to or acquisition without valid authorization of, computerized data that compromises the security, confidentiality, or integrity of personal information or private information maintained by the Village. Good faith access to, or acquisition of personal information or private information by an employee or agent of the Village for the purposes of the Village is not a breach of the security of the system, provided that the personal information or private information is not used or subject to unauthorized disclosure. In determining whether information has been accessed or acquired or is reasonably believed to have been accessed or acquired, by an unauthorized person or a person without valid authorization, the Village may consider the following factors, among others:

A. 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

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.

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 to the state Attorney General.

DEPARTMENT

Any board, committee, commission, council, department, office or other governmental entity performing a governmental or proprietary function for the Village.

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

A. Either:

(1) 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:

(a) Social security number;

(b) Driver's license number or non-driver identification card number;

(c) 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;

(d) Account number, or credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password;

(e) 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

(2) A user name or email address in combination with a password or security question and answer that would permit access to an online account.

B. Private information does not include publicly available information that is lawfully made available to the general public from Village records.

VILLAGE

The Village of Ossining, County of Westchester, State of New York.

5. **Disclosure of breach to affected persons.**

Any Village department that owns or licenses computerized data that includes private information must 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 New York State whose private information was, or is reasonably believed to have been, accessed or acquired 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 section 7 below, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The Village shall consult with the State Office of Information Technology Services to determine the scope of the breach and restoration measures.

a. 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 Village reasonably determines such exposure will not likely result in misuse of such information, or

financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the Village shall provide the written determination to the state Attorney General within ten days after the determination.

b. 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 policy shall require additional notice to those affected persons, but notice still shall be provided to the state Attorney General, the Department of State and the Office of Information Technology Services and, where appropriate, consumer reporting agencies:

(i) Regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 USC 6801-6809), as amended from time to time;

(ii) Regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) Part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) Any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

6. **Disclosure of breach to owner or licensee.**

If the Village maintains computerized data that includes private information which the Village does not own, the Village 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 or acquired by a person without valid authorization.

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.

8. **Method of notification.**

The notice required by this policy 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 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 Village; provided further that in no case shall any person or business 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 Village; or

D. Substitute notice, if the Village 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 five hundred thousand, or the Village does not have sufficient contact information. Substitute notice must include all of the following:

(1) Email notice when the Village has an email address for the subject persons;

(2) Conspicuous posting of the notice on the Village's website page; and

(3) Notification to major state-wide media.

9. **Information required.**

Regardless of the method by which notice is provided, the notice must include contact information for the Village, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft protection and protected information and a description of the categories of information that were, or are reasonably believed to have been, accessed or 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 accessed or acquired.

10. **Notification of agencies.**

A. In the event that any New York residents are to be notified of a breach of the security of the system pursuant to this policy, the Village shall notify the state Attorney General, the Department of State and the state Office of Information Technology Services as to the timing, content and distribution of the notices and the approximate number of affected people and provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.

B. In the event that more than five thousand New York residents are to be notified at one time, the Village shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected persons. Such notice must be made without delaying notice to affected New York residents.

11. **Evergreen Provision**

Any additional procedural, definitional or notification requirement which is hereafter enacted amending, repealing or otherwise affecting any of the provisions of the State Technology Law section 208 which are required of villages shall be incorporated into the provisions of this policy.