CHAPTER 22

MANDATED POLICIES

ARTICLE I – IDENTITY THEFT PROGRAM

22-1-1 PROGRAM ADOPTION. The Village developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions of 2003. 16 C.F.R. § 681.2. This Program was developed with oversight and approval of the Village. After consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities, the Village Board determined that this Program was appropriate for the Village, and therefore approved this Program on February 9, 2009.

22-1-2 PROGRAM PURPOSE AND DEFINITIONS.

(A) **Fulfilling Requirements of the Red Flags Rule.** Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

(1) Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;

(2) Detect Red Flags that have been incorporated into the Program;

(3) Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

(4) Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

(B) **Red Flags Rule Definitions Used in this Program.** The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

(1) Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

(2) Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

"Identifying information" is defined under the Rules as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

22-1-3 IDENTIFICATION OF RED FLAGS. In order to identify relevant Red Flags, the Utility considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The Utility identifies the following red flags, in each of the listed categories:

(A) **Notifications and Warnings From Credit Reporting Agencies; Red Flags.**

(1) Report of fraud accompanying a credit report;

(2) Notice or report from a credit agency of a credit freeze on a customer or applicant;

(3) Notice or report from a credit agency of an active duty alert for an applicant; and

(4) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

(B) **Suspicious Documents; Red Flags.**

(1) Identification document or card that appears to be forged, altered or inauthentic;

(2) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

(3) Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and

(4) Application for service that appears to have been altered or forged.

(C) **Suspicious Personal Identifying Information; Red Flags.**

(1) Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);

(2) Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);

(3) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

(4) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

(5) Social security number presented that is the same as one given by another customer;

(6) An address or phone number presented that is the same as that of another person;

(7) A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and

(8) A person's identifying information is not consistent with the information that is on file for the customer.

(D) **Suspicious Account Activity or Unusual Use of Account; Red Flags.**

(1) Change of address for an account followed by a request to change the account holder's name;

(2) Payments stop on an otherwise consistently up-to-date account;

(3) Account used in a way that is not consistent with prior use (example: very high activity);

(4) Mail sent to the account holder is repeatedly returned as undeliverable;

(5) Notice to the Utility that a customer is not receiving mail sent by the Utility;

(6) Notice to the Utility that an account has unauthorized activity;

(7) Breach in the Utility's computer system security; and

(8) Unauthorized access to or use of customer account information.

(E) **Alerts From Others; Red Flag.**

(1) Notice to the Utility from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

22-1-4 DETECTING RED FLAGS.

(A) **New Accounts.** In order to detect any of the Red Flags identified above associated with the opening of a **new account**, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

(1) Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;

(2) Verify the customer's identity (for instance, review a driver's license or other identification card);

(3) Review documentation showing the existence of a business entity; and

(4) Independently contact the customer.

(B) **Existing Accounts.** In order to detect any of the Red Flags identified above for an **existing account**, Utility personnel will take the following steps to monitor transactions with an account:

(1) Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);

(2) Verify the validity of requests to change billing addresses; and

(3) Verify changes in banking information given for billing and payment purposes.

22-1-5 PREVENTING AND MITIGATING IDENTITY THEFT.

(A) **Prevent and Mitigate.** In the event Utility personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

(1) Continue to monitor an account for evidence of Identity Theft;
(2) Contact the customer;
(3) Change any passwords or other security devices that permit access to accounts;
(4) Not open a new account;
(5) Close an existing account;
(6) Reopen an account with a new number;
(7) Notify the Program Administrator for determination of the appropriate step(s) to take;
(8) Notify law enforcement; or
(9) Determine that no response is warranted under the particular circumstances.

(B) **Protect Customer Identifying Information.** In order to further prevent the likelihood of Identity Theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures to protect customer identifying information:

(1) Ensure that its website is secure or provide clear notice that the website is not secure;
(2) Ensure complete and secure destruction of paper documents and computer files containing customer information;
(3) Ensure that office computers are password protected and that computer screens lock after a set period of time;
(4) Keep offices clear of papers containing customer information;
(5) Request only the last 4 digits of social security numbers (if any);
(6) Ensure computer virus protection is up to date; and
(7) Require and keep only the kinds of customer information that are necessary for utility purposes.

22-1-6 PROGRAM UPDATES. The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. In doing so, the Program Administrator will consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the Utility's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the Village Board with his or her recommended changes and the Village Board will make a determination of whether to accept, modify or reject those changes to the Program.

22-1-7 PROGRAM ADMINISTRATION.

(A) **Oversight.** Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the Utility. The Committee is headed by a Program Administrator who may be the head of the Utility or his or her appointee. Two or

more other individuals appointed by the head of the Utility or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Utility staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

(B) **Staff Training and Reports.** Utility staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

(C) **Service Provider Arrangements.** In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

(1) Require, by contract, that service providers have such policies and procedures in place; and

(2) Require, by contract, that service providers review the Utility's Program and report any Red Flags to the Program Administrator.

(D) **Non-Disclosure of Specific Practices.** For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices must be limited to the Identity Theft Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "security information" as defined in Minnesota Statutes Section 13.37 and are unavailable to the public because disclosure of them would be likely to substantially jeopardized the security of information against improper use, that use being to circumvent the Utility's Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.

ARTICLE II - USE OF SOCIAL SECURITY NUMBERS

22-2-1 DEFINITIONS.

"Person" means any individual in the employ of the Village.

"Policy" or "Privacy Policy" means this document, as now or hereafter amended.

"Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the general public.

"Social Security Number" means the nine (9) digit number assigned to an individual by the United States Social Security Administration for the purposes authorized or required under the United States Social Security Act of August 14, 1935, as amended (Public Law 74-271).

22-2-2 PROHIBITED ACTIVITIES.

(A) No officer or employee of the Village shall do any of the following:

(1) Publicly post or publicly display in any manner an individual's Social Security Number.

(2) Print an individual's Social Security Number on any card required for the individual to access products or services provided by the person or entity.

(3) Require an individual to transmit his or her Social Security Number over the Internet, unless the connection is secure or the Social Security Number is encrypted.

(4) Print an individual's Social Security Number on any materials that are mailed to the individual, through the United States Postal Service, any private mail service, electronic mail, or a similar method of delivery, unless Illinois or federal law requires the Social Security Number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, Social Security Numbers may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Illinois Unemployment Insurance Act, any material mailed in connection with any tax administered by the Illinois Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the Social Security Number. A Social Security Number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

(B) Except as otherwise provided in this policy, beginning immediately on the effective date of the Village's authorizing Ordinance, no officer or employee of the Village shall do any of the following:

(1) Collect, use, or disclose a Social Security number from an individual, unless (i) required to do so under State or Federal law, rules, or regulations, or the collection, use, or disclosure of the Social Security Number is otherwise necessary for the

performance of that agency's duties and responsibilities; (ii) the need and purpose for the Social Security Number is documented before collection of the Social Security Number; and (iii) the Social Security Number collected is relevant to the documented need and purpose.

(2) Require an individual to use his or her Social Security Number to access an Internet website.

(3) Use the Social Security Number for any purpose other than the purpose for which it was collected.

(C) The prohibitions in subsection (B) do not apply in the following circumstances:

(1) The disclosure of Social Security Numbers to agents, employees, contractors, or subcontractors of the Village or disclosure to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the officer or employee of the Village must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Policy on the Village to protect an individual's Social Security Number will be achieved.

(2) The disclosure of Social Security Numbers pursuant to a court order, warrant, or subpoena.

(3) The collection, use, or disclosure of Social Security Numbers in order to ensure the safety of: Village employees; persons committed to correctional facilities, local jails, and other law enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a Village facility.

(4) The collection, use, or disclosure of Social Security Numbers for Internal verification or administrative purposes.

(5) The collection or use of Social Security Numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit such as a pension benefit or an unclaimed property benefit.

(D) Any standards of the Village for the collection, use, or disclosure of Social Security Numbers that are stricter than the standards under this Policy with respect to the protection of those Social Security Numbers, then, in the event of any conflict with the provisions of this Policy, the stricter standards adopted by the Village shall control.

22-2-3 PUBLIC INSPECTION AND COPYING OF DOCUMENTS. Notwithstanding any other provision of this policy to the contrary, all officers and employees of the Village must comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an

individual's Social Security Number. All officers and employees of the Village must redact Social Security Numbers from the information or documents before allowing the public inspection or copying of the information or documents.

22-2-4 APPLICABIILITY.

(A) This policy does not apply to the collection, use, or disclosure of a Social Security Number as required by State or Federal law, rule, or regulation.

(B) This policy does not apply to documents that are required to be open to the public under any State or Federal law, rule, or regulation, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois.

22-2-5 COMPLIANCE WITH FEDERAL LAW. If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, the Village shall follow that law.

22-2-6 EMBEDDED SOCIAL SECURITY NUMBERS. Beginning immediately on the effective date of the Village's authorizing Ordinance, no officer or employee of the Village may encode or embed a Social Security Number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, RFID technology, or other technology, in place of removing the Social Security Number as required by this Policy.

22-2-7 IDENTITY--PROTECTION REQUIREMENTS.

(A) All officers, employees and agents of the Village identified as having access to Social Security Numbers in the course of performing their duties to be trained to protect the confidentiality of all Social Security Numbers. Training shall include instructions on the proper handling of information that contains Social Security Numbers from the time of collection through the destruction of the information.

(B) Only employees who are required to use or handle information or documents that contain Social Security Numbers have access to such information or documents.

(C) Social Security Numbers requested from an individual shall be provided in a manner that makes the Social Security Number easily redacted if required to be released as part of a public records' request.

(D) When collecting a Social Security Number or upon request by the individual, a statement of the purpose or purposes for which the Village is collecting and using the Social Security Number be provided.

(E) A written copy of this Privacy Policy, and any amendment thereto, shall be filed with the Village Board within **thirty (30) days** after approval of this Policy or any amendment thereto.

(F) The Village shall advise its employees of the existence of the Policy and make a copy of this Policy available to each employee, and shall also make this Privacy Policy available to any member of the public, upon request and at no charge for a single copy of this Privacy Policy. If the Village amends this Privacy Policy, then the Village shall also advise its employees of the existence of the amended Policy and make a copy of the amended Policy available to each employee.

22-2-8 PENALTY. Any person who violates any portion of this Article, as now or hereafter amended, shall be subject to a fine of not less than **One Hundred Dollars ($100.00)** for the first such violation and a fine of not less than **Seven Hundred Fifty Dollars ($750.00)** for each violation thereafter.

22-2-9 AMENDMENT OF PRIVACY POLICY. The Privacy Policy adopted in this Division and Chapter shall be subject to amendment from time to time by the Village Board as the Village Board shall deem necessary in its sole discretion in order to maintain the Village's compliance with the Illinois Identity Protection Act as now or hereafter amended.

22-2-10 CONFLICT WITH STRICTER LAWS. This Policy does not supersede any more restrictive law, rule, or regulation regarding the collection, use, or disclosure of Social Security Numbers.

[NOTE: This Policy is to comply with Public Act 096-9874 of the State of Illinois, cited as the Identity Protection Act, and codified as Title 30, Act 5, Section 1, et seq., as now or hereafter amended.]

ARTICLE III - FREEDOM OF INFORMATION POLICY

22-3-1 PUBLIC RECORDS AVAILABLE. To the extent required by the Freedom of Information Act, **5 ILCS 140-1 et seq.** the Village shall make available to any person for inspection or copying all public records, except as otherwise provided in Section 7 of the Freedom of Information Act, **5 ILCSA 140/7.**

22-3-2 DESIGNATION, DUTIES AND TRAINING OF FREEDOM OF INFORMATION ACT OFFICERS.

(A) The Village Administrative Assistant is hereby designated to act as Freedom of Information Officer. The Officer shall receive requests submitted to the Village under the Freedom of Information Act, insure that the Village responds to requests in a timely fashion, and issue responses under the Freedom of Information Act. The Freedom of Information officer shall develop a list of documents or categories of records that the Village shall immediately disclose upon request.

(B) Upon receiving a request for a public record, the Freedom of Information Officer shall:

(1) Note the date the Village receives the written request;

(2) Compute the date on which the period for response will expire and make a notation of that date on the written request;

(3) Maintain an electronic or paper copy of the written request including all documents submitted with the request until the request has been complied with or denied; and

(4) Create a file for the retention of the original request, a copy of the response, a record of written communications with the person making the request, and a copy of other communications regarding the request.

(C) The Freedom of Information Act officers shall successfully complete an electronic training curriculum to be developed by the Public Access Counselor in the office of the Attorney General of the State of Illinois and thereafter successfully complete an annual training program. Thereafter when a new Freedom of Information officer is designated by the Village, that person shall successfully complete the electronic training curriculum within **thirty (30) days** after assuming the position. Successful completion of the required training curriculum within the periods provided shall be a prerequisite to continue serving as a Freedom of Information officer.

22-3-3 PROCEDURES. The Village shall prominently display at the Village Clerk's office, display on its website, make available for inspection and copying, and send through the mail as requested, each of the following:

(A) A brief description of the Village, which will include, but not be limited to a block diagram giving its functional departments, the total amount of its operating budget, the number and location of all of its separate offices, the approximate number of full and part-time employees and the identification and membership of any board, commission, committee or council which operates in an advisory capacity relative to the operation of the Village, or which exercises control over its policies or procedures; and

(B) A brief description of the methods whereby the public may request information and public records, a directory designating the Freedom of Information officers, the address where request for public records should be directed, and the fees relating thereto.

22-3-4 REQUESTS TO INSPECT OR COPY. All requests to inspect or copy records or documents prepared, maintained or under the control of the Village shall be made in the following manner:

(A) All requests shall be in writing, shall state with reasonable particularity what records are to be inspected or copied, shall state whether the records are requested for a commercial purpose, and shall be signed by the person making the request. The request may be, but is not required to be, submitted on a form provided by the Village.

(B) The written request shall be submitted to the Village Clerk or to the Mayor. If neither the Village Clerk nor the Mayor is available, the request shall be submitted to any employee of the Village acting under the direction of the Village Clerk.

(C) The Officer receiving the request shall date stamp the request and indicate the date by which a response to the request must be made.

(D) Each request for other than commercial purposes shall be granted or denied in writing within **five (5) business days** after its receipt by the Village, except as hereafter stated. The failure to grant or deny a request within **five (5) business days** shall operate as a denial, except as provided hereinbelow.

(E) The time limit set forth hereinabove may be extended for an additional **five (5) business days** by notice in writing to the person making the request of the **five (5) business days** extension. The notification shall state the reason(s) for the **five (5) business day's** extension and contain a date certain on which the requested record(s) will be available. The failure to grant or deny a request within the additional **five (5) business days** shall operate as a denial. The person making the request and the Village may agree in writing to extend the time for compliance for a period to be determined by the parties. If the person making the request and the Village agree to extend the period for compliance, a failure by the Village to comply with any previous deadlines shall not be treated as a denial of the request for the records.

(F) Charges for copies of records and/or documents shall be imposed in accordance with the following:

(1) No fees shall be charged for the first **fifty (50) pages** of black and white, letter or legal sized copies requested.

(2) **Fifteen Cents ($0.15)** for one-sided page for each black and white, letter, legal sized or 11" x 17" copy requested.

(3) **One Dollar ($1.00)** for each certified copy requested.

(4) **Ten Cents ($0.10)** for each audio recording.

(G) It shall be the responsibility of the person making the request to pick up the requested documents at Village Hall. If the person making the request asks the Village to mail the documents, he or she shall provide the Village with his/her correct mailing address so as to efficiently process all requests. Copies of records requested to be mailed will be forwarded United States Certified Mail to the address provided. Pre-payment of **Two Dollars Fifty Cents ($2.50)** per ounce shall be required.

(H) When a person requests a copy of a record maintained in an electronic format, the Village shall furnish it in the electronic format specified by the person making the request, if feasible. If it is not feasible to furnish the public records in the specified electronic format, then the Village shall furnish it in the format in which it is maintained by the Village, or in paper format at the option of the person making the request.

22-3-5 REQUEST FOR COMMERCIAL PURPOSES. The Village shall respond to a request for records to be used for a commercial purpose within **twenty-one (21) working days** after receipt. The response shall (1) provide to the person making the request an estimate of the time required by the Village to provide the records requested and an estimate of the fees to be charged, which the Village may require the person to pay in full before copying the requested documents, (2) deny the request pursuant to **one (1)** or more of the exemptions set out in the Freedom of Information Act, **5 ILCS 140/1 et seq.**, (3) notify the person making the request that the request is unduly burdensome and extend an opportunity to the person making the request to attempt to reduce the request to manageable portions, or (4) provide the records requested.

Unless the records are exempt from disclosure, the Village shall comply with a commercial request within a reasonable period considering the size and complexity of the request, and giving priority to records requested for non-commercial purposes.

It is unlawful for a person to knowingly obtain a public record for a commercial purpose within disclosing that it is for a commercial purpose, and any person obtaining a public record for commercial purpose without disclosing that it is for a commercial purpose shall be fined in accordance with the Village Code.

22-3-6 FEES. The Village Clerk shall determine when the established fees are subject to waiver or reduction because the release of the requested information is in the public interest.

22-3-7 PUBLIC FILE. The Village Clerk shall establish and maintain a central file, open to the public, of all denials of requests for records which shall be indexed according to the exemption utilized to deny a request for records, and to the extent possible, according to the types of records requested.

22-3-8 GRANTING OR DENIAL OF REQUESTS. A request for all records within a category shall be granted unless the request constitutes an undue burden upon the Village. Prior to denying a request based upon the burdensome nature of the request, an opportunity to narrow the request to manageable proportions shall be provided. If the attempt to narrow the request fails, the request may be denied because compliance will unduly burden the operations of the Village and the burden outweighs the public interest in the information. The denial shall be in writing, specifying the reasons why compliance will be unduly burdensome and the extent to which compliance will so burden the operations of the Village. Repeated requests from the same person for the same records that are unchanged or identical to records previously provided are properly denied under the Freedom of Information Act shall be deemed unduly burdensome under this Section.

22-3-9 CERTAIN INFORMATION EXEMPT FROM INSPECTION AND COPYING. If any record exempt from disclosure contains material which is not exempt, the information which is exempt shall be deleted and the remaining information shall be available for inspection and copying.

22-3-10 NOTICE OF DENIAL OF REQUEST; APPEALS.

(A) If the Village denies the request, the Village shall notify the person making the request in writing of:

(1) the decision to deny the request;

(2) the reasons for the denial, including a detailed factual basis for the application of any exemption claim;

(3) the names and titles or positions of each person responsible for the denial;

(4) the right to review by the Public Access Counselor and the address and phone number for the Public Access Counselor; and

(5) the right to judicial review.

If an exemption is claimed, then the denial must include the specific reasons for the denial, including a detailed factual basis and a citation to support a legal authority.

(B) If the Village asserts an exemption under Subsection (1)(c) or (1)(f) of Section 7 of the Freedom of Information Act, it shall, within the time periods provided for Respondent to request, provide written notice to the person making the request and the Public Access Counselor of its intent to deny the request in whole or in part. The notice shall include:

(1) a copy of the request for access to records;

(2) the proposed response from the Village;

(3) a detailed summary of the Village's basis for asserting its exemption.

If the Public Access Counselor determines that further inquiry is warranted, the procedures set forth in the Freedom of Information Act, as amended from time to time, regarding the review of denials shall be applicable. Times for response compliance by the Village to the request shall be tolled until the Public Access Counselor concludes his or her inquiry.