CHAPTER 22

MANDATED POLICIES

ARTICLE I – IDENTITY THEFT PREVENTION PROGRAM

22-1-1 PURPOSE. The purpose of this Identity Theft Prevention Program (Program) is to protect customers of the Municipality's utility services from identity theft. The Program is intended to establish reasonable policies and procedures to facilitate the detection, prevention and mitigation of identity theft in connection with the opening of new Covered Accounts and activity on existing Covered Accounts.

22-1-2 SCOPE. This Program applies to the creation, modification and access to Identifying Information of a customer of one or more of the utilities operated by the Municipality (electric, natural gas, water and waste water) by any and all personnel of the Municipality, including management personnel. This Program does not replace or repeal any previously existing policies or programs addressing some or all of the activities that are the subject of this Program, but rather it is intended to supplement any such existing policies and programs.

22-1-3 DEFINITIONS. When used in this Program, the following terms have the meanings set forth opposite their name, unless the context clearly requires that the term be given a different meaning:

"Covered Account": The term "covered account" means an account that the Municipality offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments of transactions (16 CFR 681.2(b)(3)(i)). A utility account is a "covered account". The term "covered account" also includes other accounts offered or maintained by the Municipality for which there is a reasonably foreseeable risk to customers, the Municipality or its customers from identity theft (16 CFR 681.2(b)(3)(ii)).

"Identity Information": The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. Additional examples of "identifying information" are set forth in 16 CFR § 603.2(a).

"Identity Theft": The term "identity theft" means a fraud committed or attempted using the identifying information of another person without authority (16 CFR §681.2(b)(8) and 16 CFR §603.2(a)).

"Red Flag": The term "Red Flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Certain terms used but not otherwise defined herein shall have the meanings given to them in the FTC's Identity Theft Rules (16 CFR Part 681) or the Fair Credit Reporting Act of 1970 (15 U.S.C. §1681 *et seq.*), as amended by the Fair and Accurate Credit Transactions Act of 2003 into law on **December 4, 2003** (Public Law 108-159).

22-1-4 ADMINISTRATION OF THE PROGRAM. The initial adoption and approval of the Identity Theft Prevention Program shall be by Ordinance of the City Council. Thereafter, changes to the Program of a day-to-day operational character and decisions relating to the interpretation and implementation of the Program may be made by the Program Administrator. Major changes or shifts of policy positions under the Program shall only be made by the City Council.

Development, implementation, administration and oversight of the Program will be the responsibility of the Program Administrator. The Program Administrator may, but shall not be required to, appoint a committee to administer the Program. The Program Administrator shall be the head of any such committee. The Program Administrator will report at least annually to the City Council regarding compliance with this Program.

Issues to be addressed in the annual Identity Theft Prevention Report include:

(A) The effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening of new Covered Accounts and activity with respect to existing Covered Accounts.

(B) Service provider arrangements.

(C) Significant incidents involving Identity Theft and management's response.

(D) Recommendations for material changes to the Program, if needed for improvement.

22-1-5 IDENTITY THEFT PREVENTION ELEMENTS.

(A) **IDENTIFICATION OF RELEVANT RED FLAGS.** The Municipality has considered the guidelines and the illustrative examples of possible Red Flags from the FTC's Identity Theft Rules and has reviewed the Municipality's past history with instances of identity theft, if any. The Municipality hereby determines that the following are the relevant Red Flags for purposes of this Program given the relative size of the Municipality and the limited nature and scope of the services that the Municipality provides to its citizens:

(A) **Alerts, Notifications, or Other Warnings Received From Consumer Reporting Agencies or Service Providers.**

(1) A fraud or active duty alert is included with a consumer report or an identity verification response from a credit reporting agency.

(2) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

(3) A consumer reporting agency provides a notice of address discrepancy, as defined in §681.1(b) of the FTC's Identity Theft Rules.

(4) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

(a) A recent and significant increase in the volume of inquiries;

(b) An unusual number of recently established credit relationships;

(c) A material change in the use of credit, especially with respect to recently established credit relationships; or

(d) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

(B) **The Presentation of Suspicious Documents.**

(1) Documents provided for identification appear to have been altered or forged.

(2) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

(3) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

(4) Other information on the identification is not consistent with readily accessible information that is on file with the Municipality, such as a signature card or a recent check.

(5) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

(C) **The Presentation of Suspicious Personal Identifying Information, Such as a Suspicious Address Change.**

(1) Personal identifying information provided is inconsistent when compared against external information sources used by the Municipality. For example:

(a) The address does not match any address in the consumer report or CRA ID Check response; or

(b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

(2) Personal identifying information provided by the customer is not consistent with other personal identifying information

provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

(3) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Municipality. For example:
   (a) The address on an application is the same as the address provided on a fraudulent application; or
   (b) The phone number on an application is the same as the number provided on a fraudulent application.

(4) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Municipality. For example:
   (a) The billing address on an application is fictitious, a mail drop, or a prison; or
   (b) The phone number is invalid, or is associated with a pager or answering service.

(5) The SSN provided is the same as that submitted by other persons opening an account or other customers.

(6) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

(7) The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

(8) Personal identifying information provided is not consistent with personal identifying information that is on file with the Municipality.

(9) If the Municipality uses challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

(D) **The Unusual Use of, or Other Suspicious Activity Related to, the Covered Account.**

(1) Shortly following the notice of a change of address for a covered account, the Municipality receives a request for the addition of authorized users on the account.

(2) A new utility account is used in a manner commonly associated with known patterns of fraud patterns. For example: the customer fails to make the first payment or makes an initial payment but no subsequent payments.

(3) A covered account with a stable history shows irregularities.

(4) A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors.

(5) Mail sent to the customer is returned repeatedly as undeliverable although usage of utility products or services continues in connection with the customer's covered account.

(6) The Municipality is notified that the customer is not receiving paper account statements.

(7) The Municipality is notified of unauthorized usage of utility products or services in connection with a customer's covered account.

(E) **Notice of Possible Identity Theft.**

(1) The Municipality is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

22-1-6 DETECTION OF RED FLAGS. The employees of the Municipality that interact directly with customers on a day-to-day basis shall have the initial responsibility for monitoring the information and documentation provided by the customer and any third-party service provider in connection with the opening of new accounts and the modification of, or access to, existing accounts and the detection of any Red Flags that might arise. Management shall see to it that all employees who might be called upon to assist a customer with the opening of a new account or with modifying or otherwise accessing an existing account are properly trained such that they have a working familiarity with the relevant Red Flags identified in this Program so as to be able to recognize any Red Flags that might surface in connection with the transaction. An Employee who is not sufficiently trained to recognize the Red Flags identified in this Program shall not open a new account for any customer, modify any existing account or otherwise provide any customer with access to information in an existing account without the direct supervision and specific approval of a management employee. Management employees shall be properly trained such that they can recognize the relevant Red Flags identified in this Program and exercise sound judgment in connection with the response to any unresolved Red Flags that may present themselves in connection with the opening of a new account or with modifying or accessing of any existing account. Management employees shall be responsible for making the final decision on any such unresolved Red Flags.

The Program Administrator shall establish from time to time a written policy setting forth the manner in which a prospective new customer may apply for service, the information and documentation to be provided by the prospective customer in connection with an application for a new utility service account, the steps to be taken

by the employee assisting the customer with the application in verifying the customer's identity and the manner in which the information and documentation provided by the customer and any third-party service provider shall be maintained. Such policy shall be generally consistent with the spirit of the Customer Identification Program rules (31 CFR 103.121) implementing Section 326(a) of the USA PATROIT Act but need not be as detailed. The Program Administrator shall establish from time to time a written policy setting forth the manner in which customers with existing accounts shall establish their identity before being allowed to make modifications to or otherwise gain access to existing accounts.

22-1-7 RESPONSE TO DETECTED RED FLAGS. If the responsible employees of the Municipality as set forth in the previous section are unable, after making a good faith effort, to form a reasonable belief that they know the true identity of a customer attempting to open a new account or modify or otherwise access an existing account based on the information and documentation provided by the customer and any third-party service provider, the Municipality shall not open the new account or modify or otherwise provide access to the existing account as the case may be. Discrimination in respect to the opening of new accounts or the modification or access to existing accounts will not be tolerated by employees of the Municipality and shall be grounds for immediate dismissal.

The Program Administrator shall establish from time to time a written policy setting forth the steps to be taken in the event of an unresolved Red Flag situation. Consideration should be given to aggravating factors that may heighten the risk of Identity Theft, such as a data security incident that results in unauthorized access to a customer's account, or a notice that a customer has provided account information to a fraudulent individual or website. Appropriate responses to prevent or mitigate identity theft when a Red Flag is detected include:

(A) Monitoring a Covered Account for evidence of Identity Theft.

(B) Contacting the customer.

(C) Changing any passwords, security codes, or other security devices that permit access to a Covered Account.

(D) Reopening a Covered Account with a new account number.

(E) Not opening a new Covered Account.

(F) Closing an existing Covered Account.

(G) Not attempting to collect on a Covered Account or not selling a Covered Account to a debt collector.

(H) Notifying law enforcement.

(I) Determining that no response is warranted under the particular circumstances.

22-1-8 PROGRAM MANAGEMENT AND ACCOUNTABILITY.

(A) **Initial Risk Assessment - Covered Accounts.** Utility accounts for personal, family and household purposes are specifically included within the definition of "covered account" in the FTC's Identity Theft Rules. Therefore, the Municipality determines that with respect to its residential utility accounts it offers and/or maintains covered accounts. The Municipality also performed an initial risk assessment to determine whether the utility offers or maintains any other accounts for which there are reasonably foreseeable risks to customers or the utility from identity theft. In making this determination the Municipality considered (1) the methods it uses to open its accounts, (2) the methods it uses to access its accounts, and (3) its previous experience with identity theft, and it concluded that it does not offer or maintain any such other covered accounts.

(B) **Program Updates - Risk Assessment.** The Program, including relevant Red Flags, is to be updated as often as necessary but at least annually to reflect changes in risks to customers from Identity Theft. Factors to consider in the Program update include:

(1) An assessment of the risk factors identified above.

(2) Any identified Red Flag weaknesses in associated account systems or procedures.

(3) Changes in methods of Identity Theft.

(4) Changes in methods to detect, prevent, and mitigate Identity Theft.

(5) Changes in business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

(C) **Training and Oversight.** All staff and third-party service providers performing any activity in connection with one or more Covered Accounts are to be provided appropriate training and receive effective oversight to ensure that the activity is conducted in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

22-1-9 OTHER LEGAL REQUIREMENTS. Awareness of the following related legal requirements should be maintained:

(A) 31 U.S.C. 5318 (g) - Reporting of Suspicious Activities

(B) 15 U.S.C. 1681 c-1 (h) - Identity Theft Prevention; Fraud Alerts and Active Duty Alerts - Limitations on Use of Information for Credit Extensions

(C) 15 U.S.C. 1681 s-2 - Responsibilities of Furnishers of Information to Consumer Reporting Agencies

(D) 15 U.S.C. 1681 m - Requirements on Use of Consumer Reports

(Ord. No. 08-29; 10-27-08)

ARTICLE II – POLICY PROHIBITING SEXUAL HARASSMENT

22-2-1 PROHIBITION ON SEXUAL HARASSMENT. It is unlawful to harass a person because of that person's sex. The courts have determined that sexual harassment is a form of discrimination under Title VII of the U.S. Civil Rights Act of 1964, as amended in 1991. All persons have a right to work in an environment free from sexual harassment. Sexual harassment is unacceptable misconduct which affects individuals of all genders and sexual orientations. It is a policy of this City to prohibit harassment of any person by any municipal official, municipal agent, municipal employee or municipal agency or office on the basis of sex or gender. All municipal officials, municipal agents, municipal employees and municipal agencies or offices are prohibited from sexually harassing any person, regardless of any employment relationship or lack thereof.

22-2-2 DEFINITION OF SEXUAL HARASSMENT. This policy adopts the definition of sexual harassment as stated in the Illinois Human Rights Act, which currently defines sexual harassment as:

(A) Any unwelcome sexual advances or requests for sexual favors or any conduct of a sexual nature when:

(1) Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment,

(2) Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; or

(3) Such conduct has the purpose or effect of substantially interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment.

(B) Conduct which may constitute sexual harassment includes:

(1) **Verbal.** Sexual innuendoes, suggestive comments, insults, humor, and jokes about sex, anatomy or gender-specific traits, sexual propositions, threats, repeated requests for dates, or statements about other employees, even outside their presence, of a sexual nature.

(2) **Non-verbal.** Suggestive or insulting sounds (whistling), leering, obscene gestures, sexually suggestive bodily gestures, "catcalls", "smacking" or "kissing" noises.

(3) **Visual.** Posters, signs, pin-ups or slogans of a sexual nature, viewing pornographic material or websites.

(4) **Physical.** Touching, unwelcome hugging or kissing, pinching, brushing the body, any coerced sexual act or actual assault.

(5) **Textual/Electronic.** "Sexting" (electronically sending messages with sexual content, including pictures and video), the use of sexually explicit language, harassment, cyber stalking or threats via all forms of electronic communication (e-mail, text/picture/ video messages, intranet/on-line postings, blogs, instant messages and social network websites like Facebook and Twitter).

(C) The most severe and overt forms of sexual harassment are easier to determine. On the other end of the spectrum, some sexual harassment is more subtle and

depends, to some extent, on individual perception and interpretation. The courts will assess sexual harassment by a standard of what would offend a "reasonable person."

22-2-3 PROCEDURE FOR REPORTING AN ALLEGATION OF SEXUAL HARASSMENT.

(A) An employee who either observes sexual harassment or believes herself/himself to be the object of sexual harassment should deal with the incident(s) as directly and firmly as possible by clearly communicating his/her position to the offending employee, and his/her immediate supervisor. It is not necessary for sexual harassment to be directed at the person making the report.

(B) Any employee may report conduct which is believed to be sexual harassment, including the following:

(1) **Electronic/Direct Communication.** If there is sexual harassing behavior in the workplace, the harassed employee should directly and clearly express his/her objection that the conduct is unwelcome and request that the offending behavior stop. The initial message may be verbal. If subsequent messages are needed, they should be put in writing in a note or a memo.

(2) **Contact with Supervisory Personnel.** At the same time direct communication is undertaken, or in the event the employee feels threatened or intimidated by the situation, the problem must be promptly reported to the immediate supervisor of the person making the report, a department head, a director of human resources, an ethics officer, the city manager or administrator, or the chief executive officer of the Municipality.

The employee experiencing what he or she believes to be sexual harassment must not assume that the employer is aware of the conduct. If there are no witnesses and the victim fails to notify a supervisor or other responsible officer, the Municipality will not be presumed to have knowledge of the harassment.

(3) **Resolution Outside Municipality.** The purpose of this policy is to establish prompt, thorough and effective procedures for responding to every report and incident so that problems can be identified and remedied by the Municipality. However, all municipal employees have the right to contact the Illinois Department of Human Rights (IDHR) or the Equal Employment Opportunity Commission (EEOC) for information regarding filing a formal complaint with those entities. An IDHR complaint must be filed within **three hundred (300) days** of the alleged incident(s) unless it is a continuing offense. A complaint with the EEOC must also be filed within **three hundred (300) days**.

(C) Documentation of any incident may be submitted with any report (what was said or done, the date, the time and the place), including, but not limited to, written records such as letters, notes, memos and telephone messages.

(D) All allegations, including anonymous reports, will be accepted and investigated regardless of how the matter comes to the attention of the Municipality. However, because of the serious implications of sexual harassment charges and the difficulties associated

with their investigation and the questions of credibility involved, the claimant's willing cooperation is a vital component of an effective inquiry and an appropriate outcome.

22-2-4 PROHIBITION ON RETALIATION FOR REPORTING SEXUAL HARASSMENT ALLEGATIONS.

(A) No municipal official, municipal agency, municipal employee or municipal agency or office shall take any retaliatory action against any municipal employee due to a municipal employee's:

(1) Disclosure or threatened disclosure of any violation of this policy,

(2) The provision of information related to or testimony before any public body conducting an investigation, hearing or inquiry into any violation of this policy, or

(3) Assistance or participation in a proceeding to enforce the provisions of this policy.

(B) For the purposes of this policy, retaliatory action means the reprimand, discharge, suspension, demotion, denial of promotion or transfer, or change in the terms or conditions of employment of any municipal employee that is taken in retaliation for a municipal employee's involvement in protected activity pursuant to this policy.

(C) No individual making a report will be retaliated against even if a report made in good faith is not substantiated. In addition, any witness will be protected from retaliation.

(D) Similar to the prohibition against retaliation contained herein, the State Officials and Employees Ethics Act **(5 ILCS 430/15-10)** provides whistleblower protection from retaliatory action such as reprimand, discharge, suspension, demotion, or denial of promotion or transfer that occurs in retaliation for an employee who does any of the following:

(1) Discloses or threatens to disclose to a supervisor or to a public body an activity, policy, or practice of any officer, member, State agency, or other State employee that the State employee reasonably believes is in violation of a law, rule, or regulation;

(2) Provides information to or testifies before any public body conducting an investigation, hearing, or inquiry into any violation of a law, rule, or regulation by any officer, member, State agency or other State employee; or

(3) Assists or participates in a proceeding to enforce the provisions of the State Officials and Employees Ethics Act.

(E) Pursuant to the Whistleblower Act **(740 ILCS 174/15(a))**, an employer may not retaliate against an employee who discloses information in a court, an administrative hearing, or before a legislative commission or committee, or in any other proceeding, where the employee has reasonable cause to believe that the information discloses a violation of a State or federal law, rule, or regulation. In addition, an employer may not retaliate against an employee for disclosing information to a government or law enforcement agency, where the employee has reasonable cause to believe that the information discloses a violation of a State or federal law, rule, or regulation. **(740 ILCS 174/15(b))**.

(F) According to the Illinois Human Rights Act **(775 ILCS 5/6-101)**, it is a civil rights violation for a person, or for two or more people to conspire, to retaliate against a person because he/she has opposed that which he/she reasonably and in good faith believes to be sexual harassment in employment, because he/she has made a charge, filed a complaint,

testified, assisted, or participated in an investigation, proceeding, or hearing under the Illinois Human Rights Act.

(G) An employee who is suddenly transferred to a lower paying job or passed over for a promotion after filing a complaint with IDHR or EEOC, may file a retaliation charge – either due within **three hundred (300) days** of the alleged retaliation.

22-2-5 CONSEQUENCES OF A VIOLATION OF THE PROHIBITION ON SEXUAL HARASSMENT. In addition to any and all other discipline that may be applicable pursuant to municipal policies, employment agreements, procedures, employee handbooks and/or collective bargaining agreement, any person who violates this policy or the Prohibition on Sexual Harassment contained in **5 ILCS 430/5-65**, may be subject to a fine of up to **Seven Hundred Fifty Dollars ($750.00)** per offense, applicable discipline or discharge by the Municipality and any applicable fines and penalties established pursuant to local ordinance, State law or Federal law. Each violation may constitute a separate offense. Any discipline imposed by the Municipality shall be separate and distinct from any penalty imposed by an ethics commission and any fines or penalties imposed by a court of law or a State or Federal agency.

22-2-6 CONSEQUENCES FOR KNOWINGLY MAKING A FALSE REPORT. A false report is a report of sexual harassment made by an accuser using the sexual harassment report to accomplish some end other than stopping sexual harassment or retaliation for reporting sexual harassment. A false report is not a report made in good faith which cannot be proven. Given the seriousness of the consequences for the accused, a false or frivolous report is a severe offense that can itself result in disciplinary action. Any person who intentionally makes a false report alleging a violation of any provision of this policy shall be subject to discipline or discharge pursuant to applicable municipal policies, employment agreements, procedures, employee handbooks and/or collective bargaining agreements.

In addition, any person who intentionally makes a false report alleging a violation of any provision of the State Officials and Employees Ethics Act to an ethics commission, an inspector general, the State Police, a State's Attorney, the Attorney General, or any other law enforcement official is guilty of a Class A misdemeanor. An ethics commission may levy an administrative fine of up to **Seven Hundred Fifty Dollars ($750.00)** against any person who intentionally makes a false, frivolous or bad faith allegation.

(Ord. No. 18-21; 11-13-18)