CHAPTER 22

MANDATED POLICIES

ARTICLE I – IDENTITY THEFT PREVENTION PROGRAM

22-1-1 PURPOSE. The purpose of this Identity Theft Prevention Program hereinafter referred to as "Program" is to protect customers of the City'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 City, referred to herein as "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:

(A) ***"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)).

(B) ***"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)).

(C) ***"Identifying 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 of 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).

(D) ***"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. 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 City Administrator hereinafter referred to as "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 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:

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

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

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

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

(d) 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:

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

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

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

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

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

(a) 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.

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

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

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

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

(b) 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.

(c) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Municipality. For example:

(i) The address on an application is the same as the address provided on a fraudulent application; or

(ii) The phone number on an application is the same as the number provided on a fraudulent application.

(d) 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:

(i) The billing address on an application is fictitious, a mail drop, or a prison; or

(ii) The phone number is invalid, or is associated with a pager or answering service.

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

(f) 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.

(g) 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.

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

(i) 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.

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

(a) 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;

(b) 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;

(c) A covered account with a stable history shows irregularities;

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

(e) 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;

(f) The Municipality is notified that the customer is not receiving paper account statements;

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

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

(B) **Detection of Red Flags.** The employees of the Municipality that interact 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 an 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 for 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 PATRIOT 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 existing accounts.

(C) **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:

(1) Monitoring a Covered Account for evidence of Identity Theft.
(2) Contacting the customer.

(3) Changing any passwords, security codes, or other security devices that permit access to a Covered Account.
(4) Reopening a Covered Account with a new account number.
(5) Not opening a new Covered Account.
(6) Closing an existing Covered Account.
(7) Not attempting to collect on a Covered Account or not selling a Covered Account to a debt collector.
(8) Notifying law enforcement.
(9) Determining that no response is warranted under the particular circumstances.

22-1-6 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.

22-1-7 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 a Consumer Reports

(Ord. No. 1204; 03-02-09)

ARTICLE II – POLICY AGAINST DISCRIMINATION, HARASSMENT AND SEXUAL MISCONDUCT

22-2-1 STATEMENT OF POLICY. It is the City's policy that it will not tolerate or condone discrimination or harassment on the basis of race, color, religion, creed, sex, gender-identity, gender-expression, sexual orientation, pregnancy, childbirth, medical or common conditions relating to pregnancy and childbirth, genetic information, national origin, age, physical or mental disability, ancestry, marital status, military status, arrest record, unfavorable discharge from military service, order of protection status, citizenship status or any other classification protected under federal or state law. Sexual misconduct is also prohibited. The City will neither tolerate nor condone discrimination, harassment or sexual misconduct by employees, managers, supervisors, elected officials, co-workers, or non-employees with whom City has a business, service, or professional relationship. "Employee," for purposes of this policy only, includes any individual performing work for City, an apprentice, an applicant for apprenticeship, or an unpaid intern. The City has appointed an ethics officer to receive and oversee investigations of complaints made pursuant to this policy and he/she is referred to in this policy as City's "Ethics Officer." The Ethics Officer's contact information can be obtained from your supervisor and is posted at City Hall. The City reserves the right to change the Ethics Officer from time to time.

Retaliation against an employee who complains about or reports any act of discrimination, harassment or misconduct in violation of this policy is prohibited. Retaliation against any employee who participates in an investigation pursuant to this policy is likewise prohibited. The City is committed to ensuring and providing a work place free of discrimination, harassment, sexual misconduct and retaliation. The City will take disciplinary action, up to and including termination, against an employee who violates this policy.

As set forth above, sexual harassment and sexual misconduct are prohibited. Sexual harassment includes unwelcome sexual advances, requests for sexual favors, or any other visual, verbal or physical conduct of a sexual nature when:

(A) submission to or rejection of this conduct explicitly or implicitly affects a term or condition of individual's employment;

(B) submission to or rejection of the conduct is used as the basis for an employment decision affecting the harassed employee; or

(C) the harassment has the purpose or effect of unreasonably interfering with the employee's work performance or creating an intimidating, hostile or offensive work environment because of the persistent, severe or pervasive nature of the conduct.

22-2-2 CIRCUMSTANCES FOR SEXUAL HARASSMENT. Sexual harassment can occur in a variety of circumstances, including but not limited to the following:

(A) The employee as well as the harasser may be a woman or a man. The employee does not have to be of the opposite sex.

(B) The harasser can be the employee's supervisor, an agent of the employer, a supervisor in another area, a co-worker, or a non-employee.

(C) The employee does not have to be the person harassed but could be anyone affected by the offensive conduct.

(D) Unlawful sexual harassment may occur without economic injury to or discharge of the employee.

(E) The harasser's conduct must be unwelcome.

22-2-3 EMPLOYEE CONDUCT. Each employee musts exercise his or her own good judgment to avoid engaging in conduct that may be perceived by others as sexual harassment or harassment based on any status protected by law. The following are illustrations of actions that the City deems inappropriate and in violation of our policy:

(A) Unwanted sexual advances.

(B) Offering employment benefits in exchange for sexual favors.

(C) Retaliating or threatening retaliation after a negative response to a sexual advance or after an employee has made or threatened to make a harassment complaint.

(D) Visual conduct such as leering, making sexual gestures, displaying sexually suggestive objects or pictures, cartoons, calendars or posters.

(E) Verbal conduct such as making derogatory comments, using epithets or slurs, making sexually explicit jokes or suggestive comments about a person's body or dress.

(F) Written or electronic communications of a sexual nature or containing statements or images which may be offensive to individuals in a particular protected group, such as racial or ethnic stereotypes or stereotypes about disabled individuals.

(G) Physical conduct such as unwanted touching, assaulting, impeding or blocking movements.

Sexual misconduct is strictly prohibited by the City and can include any inappropriate and/or illegal conduct of a sexual nature including, but not limited to, sexual abuse, sexual exploitation, sexual intimidation, rape, sexual assault, or ANY sexual contact or sexual communications with a minor (including, but not limited to, conduct or communications which are written, electronic, verbal, visual, virtual or physical).

22-2-4 RESPONSIBILITIES.

(A) **Supervisors.** Each supervisor shall be responsible for ensuring compliance with this policy, including the following:

(1) Monitoring the workplace environment for signs of discrimination, harassment or sexual misconduct;

(2) Immediately notifying law enforcement where there is reasonable belief that the observed or complained of conduct violates the criminal laws of the State of Illinois.

(3) Immediately notifying the Department of Children and Family Services (DCFS) Hotline (1-800-25-ABUSE or 1-800-252-2873) if the observed or complained of conduct involves the abuse of a minor.

(4) Immediately stopping any observed acts of discrimination, harassment or sexual misconduct and taking appropriate steps to intervene, whether or not the involved employees are within his/her line of supervision;

(5) Immediately reporting any complaint of harassment, discrimination or sexual misconduct to the City Attorney or to the Ethics Officer, and;

(6) Taking immediate action to limit the work contact between the individuals when there has been a complaint of discrimination, harassment or sexual misconduct, pending investigation.

(B) **Employees.** Each employee is responsible for assisting in the prevention of discrimination, harassment or sexual misconduct through the following acts:

(1) Refraining from participation in, or encouragement of, actions that could be perceived as discrimination, harassment or sexual misconduct;

(2) Immediately reporting any violations of this policy to a supervisor, the Ethics Officer, or City Attorney and law enforcement (if appropriate under the circumstances) and/or DCFS (if appropriate under the circumstances); Employees are obligated to report violations of this policy as soon as they occur. An employee should not wait until the conduct becomes unbearable before reporting the prohibited conduct. All employees are obligated to report instances of prohibited conduct even if the conduct is merely observed and directed toward another individual and even if the other person does not appear to be bothered or offended by the conduct. All employees are obligated to report instances of prohibited conduct regardless of the identity of the alleged offender (e.g. man, woman, supervisor, elected official, co-worker, volunteer, vendor, member of public).

(3) Encouraging any employee who confides that he/she is the victim of conduct in violation of this policy to report these acts to a supervisor.

Failure to take action to stop known discrimination, harassment or sexual misconduct may be grounds for discipline.

There is a clear line most cases between a mutual attraction and a consensual exchange and unwelcome behavior or pressure for an intimate relationship. A friendly interaction between two persons who are receptive to one another is not considered unwelcome or harassment. Employees are free to form social relationships of their own choosing. However, when one employee is pursuing or forcing a relationship upon another who does not like or want it, regardless of friendly intentions, the behavior is unwelcome sexual behavior. An employee confronted with these actions is encouraged to inform the harasser that such behavior is offensive and must stop. You should assume that sexual comments are unwelcome unless you have clear unequivocal indications to the contrary. In other words, another person does not have to tell you to stop for your conduct to be harassment and unwelcome. Sexual communications and sexual contact with a minor are ALWAYS prohibited.

If you are advised by another person that your behavior is offensive, you must immediately stop the behavior, regardless of whether you agree with the person's perceptions of your intentions.

The City does not consider conduct in violation of this policy to be within the courage and scope of employment and does not sanction such conduct on the part of any employee, including supervisory and management employees.

22-2-5 APPLICABLE PROCEDURES. The City takes allegations of discrimination, harassment and sexual misconduct very seriously. It will actively investigate all complaints.

It is helpful for the employee to directly inform the offending individual that the conduct is unwelcome and must stop. The employee should use the City's complaint procedure to advise the City of any perceived violation of this policy as soon as it occurs.

(A) **Bringing a Complaint.** Any employee of the City, or any other person, who believes that there has been a violation of this policy may bring the matter to the attention of the City in one of the following ways:

(1) Advising his or her supervisor or the Ethics Officer for the City; or

(2) Advising the offending employee's supervisor, the City Attorney or the Mayor's Administrative Assistant in the event that the alleged harasser is the City Attorney.

If the complaint involves someone in the employee's direct line of command, then the employee should go directly to the City Attorney or the Ethics Officer.

The complaint should be presented as promptly as possible after the alleged violation of this policy occurs.

The City will take steps to ensure that complaints made are kept confidential to the extent permissible under the law. Individuals who are involved in an investigation under this policy are required to keep the matter confidential to the fullest extent permitted under the law.

(B) **Resolution of a Complaint.** Promptly after a complaint is submitted, the City will undertake such investigation, corrective and preventive actions as are appropriate. In general, the procedure in resolving any complaints can (but will not necessarily) include any of the following items:

(1) A meeting between the employee making the complaint and an individual designated by the City to investigate such complaints. Important data to be provided by the complaining employee includes the following:

(a) A description of the specific offensive conduct;

(b) Identification of all person(s) who engaged in the conduct;

(c) The location where the conduct occurred;

(d) The time when the conduct occurred;

(e) Whether there were any witnesses to the conduct;

(f) Whether conduct of a similar nature has occurred on prior occasions;

(g) Whether there are any documents which would support the complaining employee's allegations;

(h) What impact the conduct had on the complaining employee.

(2) While not required, the City encourages anyone who makes a complaint under this policy to provide a written statement setting forth the above details and attaching any pertinent records.

(3) After a complaint is submitted by the employee, the alleged offending individual should be contacted by a designated representative of the City. The alleged offending individual should be advised of the charges brought against him or her, and may be provided with a copy of the written statement of complaint made by the complaining employee (if applicable). The alleged offending individual should have an opportunity to fully explain his or her side of the circumstances, and may also submit a written statement, if desired.

(4) After the alleged offending individual is interviewed, any witnesses identified by either the complaining employee or the alleged offending individual may be interviewed separately.

(5) Once this investigation is completed, the City will take such action as is appropriate based upon the information obtained in the investigation. In the event that the City finds merit in the charges made by the complaining employee, disciplinary action will be taken against the offending employee. This disciplinary action may, but need not necessarily, include:
   (a) Verbal or written reprimand;
   (b) Placing the offending employee on a corrective action plan for a period of time to be identified;
   (c) Delay in pay increases or promotions;
   (d) Suspending the offending employee from work without pay;
   (e) Demotion;
   (f) Immediate termination.

(6) Upon completion of the investigation, the City will advise the complaining employee of the results of the investigation, including action taken, if any, against the offending individual.

When investigating alleged violations of this policy, the City looks at the whole record including, but not limited to, the nature of the allegations, the context in which the alleged incidents occurred, and the statements of the parties and witnesses. A determination on the allegations is made from the facts on a case-by-case basis.

22-2-6 NON-RETALIATION. Under no circumstances will there be any retaliation against any employee making a complaint of discrimination, harassment or sexual misconduct. Any act of retaliation by any party directed against a complaining employee, an accused employee, witnesses, or participants in the process will be treated as a separate and distinct complaint and will be similarly investigated. Complaints of retaliation should be addressed to the Ethics Officer or City Attorney. Illinois law provides protections to whistleblowers as set forth in the Whistleblower Act, **740 ILCS 174/15** and the Illinois Human Rights Act, **775 ILCS 5/6-101**.

22-2-7 FALSE REPORTS PROHIBITED. It is a violation of this policy for an employee to knowingly make a false report of discrimination, harassment, sexual misconduct, or retaliation. An employee who is found to have knowingly made a false report is subject to disciplinary action, as set forth in **Section 22-2-5(B)(5)** above.

22-2-8 ADDITIONAL RESOURCES. If you have any questions concerning the City's policies on this matter, please see your supervisor, the Ethics Officer, or the City Attorney. Further information may also be obtained from the Illinois Department of Human Rights, 312-814-6200 or the Equal Employment Opportunity Commission (EEOC), 800-669-4000. Confidential reports of harassment or discrimination may also be filed with these state agencies. For matters involving the abuse of minors the Illinois Department of Children and Family Services (DCFS) may be contacted by dialing 800-25-ABUSE.

Please acknowledge receipt and review of this policy by completing the acknowledgement form at the end of this policy and returning it to the Mayor's Administrative Assistant.

(Ord. No. 1392; 01-02-18)