Personnel and Administrative Policy and Procedure

SUBJECT: Identity Theft Prevention Program (ITPP)	**EFFECTIVE DATE:** May 1, 2009 **REVIEWED:** **REVISED:** December 2012
CATEGORY: 200 **POLICY NUMBER: 200.27**	**CROSS REFERENCE:**

Purpose: To set forth the purposeful protection of personal information in compliance with the Oregon Consumer Identity Theft Protection Act (2007) and the Fair and Accurate Credit Transactions (FACT) Act (2003), and to implement a Program for detection, prevention and mitigation of Identity Theft in connection with municipal utilities and other deferred payment accounts, as set forth by the Federal Trade Commission Red Flag Rules (2007).

Policy: City employees are responsible for protecting personal information from unauthorized access. Access to personal information shall be restricted to a "need-to-know" basis and be available only to those individuals authorized to use such information as part of their duties and with the requirement that they keep the information confidential and use it only for authorized business purposes.

Departments that collect and store personal data shall develop written procedures to help prevent, detect, and respond to Identity Theft of consumer account information through identification of "Red Flags".

Definitions:

Identity Theft: The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person."

Personal or Identifying information: For these purposes personal information will be considered a person's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or data elements are not encrypted or when the data elements are encrypted and the encryption key also has been acquired, or when either the name or the data elements are not redacted:

- Social Security number
- Driver's license number or state identification card number
- Identification number issued by a foreign nation
- Passport number or other United States issued identification number
- Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account.
- Date of birth
- Alien Registration Number
- Employee or Tax Identification Number
- Computer Internet Provider Protocol Address or Routing Code

Red Flags: A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft, including but not limited to:

- Notification and warnings from credit reporting agencies

- Suspicious documents (i.e. documents that appear to be forged, inauthentic, or altered)
- Notice from law enforcement authorities or victims of identity theft about possible compromise of covered accounts
- Suspicious personal identifying information
- Suspicious account activity
- Unusual use of account.

Scope: All City employees are required to adhere to the ITPP policies with respect to preventing Identity Theft. The policies apply both when handling City employee and/or city resident data, and include existing accounts as well as accounts to be opened that are covered under the Red Flag Rules. The ITPP guidelines, policies, and scope encompass both the State of Oregon requirements and the Red Flag requirements under the United States Code.

Guidelines

- The Program shall be adopted by City Council.
- The Records and Information Management Director is designated as the Program Administrator to coordinate implementation of the ITPP Information Security Program with the Information Security Program Coordinator ("ISPC"), and the department directors.
- Each department must put in writing procedures to meet the requirements of this policy and place those procedures on file with the Program Administration as coordinator of this Program.

Responsibilities

Information Security Program Coordinator

- Monitor procedures developed by departments to ensure compliance.
- Retain procedures and make available to other employees and any citizens that may request such information.

Department directors

- Ensure that procedures are established for all personal data as outlined under the guidelines section.

Supervisors

- Audit department operations and note when personal data is being gathered and how it is being stored and disposed of.
    - Inventory all computers, laptops, disks and other equipment to note where and how personal data is being stored. Make sure all storage is secured.
- Scale down any collection of personal data where possible. For example employee numbers have been changed from using the last four digits of a person's social security number to a randomly generated number.
    - Audit forms and procedures to determine how the data is being collected and handled.
    - Eliminate any unnecessary collection and transmission of data.
    - Use social security numbers only for required and lawful purposes such as payroll reporting of employee taxes.
- Make sure there are proper protections and locks on all stored data whether stored in hard copy or electronic format.
- Properly dispose of any stored personal data that is no longer needed.
- Train all employees on the proper collection and storage of personal information collected by your department.

All Employees

Data Collection: When collecting any protected personal information from an employee or citizen, implement and maintain reasonable safeguards to protect the security and confidentiality of the information. This also includes the proper disposal of information.

- Be knowledgeable of agency safeguards and follow all procedures and processes established to protect information assets and personal information.
- Protect personal information from unauthorized viewing.
- Properly secure personal information both when in use and when stored. This includes when filed electronically or in printable format (such as paper, discs, and removable storage devices).
- Obtain written permission to transport personal information outside of the physical boundaries of City facilities. This includes not storing data on portable computers or storage devices that will be taken outside of City facilities, unless there is a business necessity for doing so such as mobile data terminals in Police cars.
- Encrypt personal information when appropriate and feasible.
- Have a valid business purpose to send personal information over the network. Only use secure networks to transmit information.
- Have prior written approval to download personal information to any portable or removable device.
- Only use the last 4 numbers of an identifying document when possible. For example, only record the last 4 digits of the ID (such as driver's license) presented when notarizing someone's documents.
- Do not print Social Security numbers on cards or documents mailed or publicly displayed or otherwise post a social security number. Exceptions include requirements to complete and process W2s, W4s, and other records that are required by law to be made available to the public, for use of internal verification or administrative processes, for legal requirements, or for enforcing a judgment or court order.
    - Other exceptions include: Rules adopted by the courts and copies of records possessed by a court, the State court Administrator or the Secretary of State.

Specific Program Elements and Confidentiality

For the effectiveness of the ITPP, the Red Flag Rule envisions a degree of confidentiality regarding the City's specific practices relating to Identity Theft detection, prevention, and mitigation. Therefore, under this Program, knowledge of such specific practices are to be limited to the ISPC or any committee formed pursuant to the Red Flag Rules, and those employees who need to know them for purposes of identifying Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general Red Flag detection, implementation and prevention practices as specifically required by the Red Flag Rules are shown in this document.

II. ITPP IMPLEMENTATION

This ITPP was developed with oversight and approval of the Milwaukie City Council. It is the policy of the City of Milwaukie to protect personal information by complying with the legal authorities acknowledged above. After consideration of the size and complexity of the City's utility services operations and account systems (the "Utility"), in conjunction with the security procedures implemented earlier in response to State of Oregon and Federal rules, and particularly the nature and scope of the

Utility's activities, the City Council determined that this Program was appropriate for the City of Milwaukie, and therefore adopted this Program on April 21, 2009.

A. Fulfilling Requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor, in this case the City of Milwaukie as a provider and collector of fees for certain utilities, 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 to customers or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule Definitions Used in This Program

"Identity Theft" and "Personal or Identifying Information" are defined at the beginning of this document under I. IMPLEMENTATION. Definitions.

According to the Red Flags 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 above under Definitions, Personal or Identifying Information".

III. 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);
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 Flags

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

IV. 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.

Detect

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 cards);
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 within an account:

Detect

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.

V. PREVENTING AND MITIGATING IDENTITY THEFT

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, in accordance with other department operating procedures.

Prevent and Mitigate

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.

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 in conjunction with 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.

VI. NOTIFICATION OF A BREACH

- Employees must immediately report any suspected breach of personal information to a supervisor.
- The City must notify any affected party as to which files were affected and what personal information has been subject to a security breach.

Risk Manager and HR Director:

- In the event of a possible breach, the risk manager and HR director will in consultation with Council, investigate to determine the severity of the potential harm, including assessment of the confidential information involved, potential victims, and level of risk. An action plan will be developed based on the findings.

VII. PROGRAM UPDATES

The Program Administrator will periodically review and update this Program and if necessary internal procedures 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 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 City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

VIII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the City Manager, who 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 with 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. Training will occur with designated employees on a need to know basis according to job responsibilities and be documented in the personnel file upon employment, and on an on-going basis to ensure employees are kept up-to-date on new issues. Staff will provide reports to the Program and the effectiveness of the Program.

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. Responding to Notices of Address Discrepancies.

1. The City of Milwaukie will furnish a confirmed address to the consumer reporting agency (CRA) under the following conditions:

   - The City of Milwaukie can form a reasonable belief the customer report relates to the customer in the City of Milwaukie's records.
   - The customer under review is a current customer with an active account.
   - The request involves a customer opening a new account.
   - CRA provides the request in writing.
   - Utility has established a relationship with the CRA.

2. Confirmation of address will be provided by the City of Milwaukie to CRA in writing within 14 days of request.

E. Properly Handling Reports of Suspected Identity Theft.

1. When a customer suspects Identity Theft, they must notify the City of Milwaukie in writing, completing the Federal Trade Commission ("FTC") Affidavit. Instructions for completion are a part of the form.
2. The Customer must submit a copy of affidavit with police report to the City of Milwaukie.
3. Customer Service staff will make a copy of the customer's photo ID and record the receipt of the documents.
4. Copies of the FTC affidavit, police report and photo ID will be submitted to the City of Milwaukie to ensure reporting to proper organizations.

F. Conducting Information Technology Audits to Monitor Risk for Identity Theft.

1. The City of Milwaukie will develop a Program checklist to audit and evaluate internal and external Identity Theft risk in information technology security.

G. Ensuring the Confidentiality of Medical Records.

1. The City of Milwaukie will treat all medical information pertaining to the customer as confidential.
2. Medical information is information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer that relates to:
   - The past, present, or future physical, mental, or behavioral health care to an individual;
   - The provision of health care to an individual; or
   - The payment for the provision of health care to an individual.
3. Medical information will not be used in the determination of a customer's eligibility for services.
4. The City of Milwaukie will not release medical information to third parties.

5. Rescue squads and government entities that require the location of citizens on ventilators for planning purposes will be provided the information upon the written permission of the customer.

H. Disposal of records under protective procedures.

1. The City of Milwaukie will collect and protect documents and data through the appropriate retention periods, until the time of destruction.
    - Paper including Faxes: The exposure of customer's secured information in the office will be monitored by the City of Milwaukie management. Examples are shredding any documents containing secured information before disposal and locking documents in secured storage until disposal time.
    - Electronic records will be erased.
    - Compact disks (CDs) will be broken.
2. The City of Milwaukie will maintain records of data destruction to include content, date and method of destruction.
3. The destruction of records will be scheduled no longer than on a monthly basis to minimize possible exposure of information as well as excess storage of records.

On a continual basis, the city shall review any new regulations or criteria on the issue of Identity Theft Prevention and make any necessary changes to the rules and procedures created to detect, prevent, and mitigate Identity Theft.