GLENDALE WATER AND POWER
IDENTITY THEFT PREVENTION PROGRAM
(In Accordance with the Fair and Accurate Credit Transaction Act of 2003)

I. Purpose and Scope of Identity Theft Program

A. Glendale Water & Power (GWP) recognizes the responsibility to safeguard personal customer information within the workplace. The goal of this policy is to detect, prevent, and mitigate identity theft utilizing guides set forth in the FACT ACT (2003) and to provide for continued administration of the Program.

B. This Policy applies to all employees, contractors, consultants, and temporary workers within GWP or the City who have access to Customer Service Division's (CSD) information.

C. This Policy helps to protect employees, customers, and the City from damages related to loss or misuse of sensitive information.

II. Program Administration

A. The General Manager of Glendale Water & Power is responsible for the administration of the Identity Theft Prevention Program and will approve any updates or changes.

B. The Assistant General Manager of Customer and Support Services will provide general oversight.

C. The Customer Services Administrator is designated as the Privacy Officer.

D. Employees with access to CSD information shall receive two hours of initial training and a minimum of 30 minutes refresher training annually.

III. Definitions

A. **Covered Account** means:

1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account**, utility account**, checking account, or savings account; and

2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. **Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.

C. **Identifying Information** means an individual's first name or first initial and last name with any of the following:

   a. Social Security number
   b. Driver's license number or State Issued Identification Card number, or
   c. Account number, credit or debit card number, in combination with something like a PIN or password which would allow access to the account.

D. **Identity theft** means fraud committed or attempted using the identifying information of another person without authority.

E. **Red flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

IV. General Policy

Personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.

A. Hard Copy Distribution

Each employee and contractor will comply with the following:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with identifying information will be locked when not in use.

2. Storage rooms containing documents with identifying information and record retention areas will be locked at the end of each workday or when unsupervised.

3. Desks, workstations, work areas, printers, and fax machines, and common shared work areas will be cleared of all documents containing identifying information when not in use.

4. When documents containing identifying information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut shredding device.

5. Documents containing identifying information and prepared for external mail will be placed in a sealed envelope prior to being delivered to the mail room. Documents prepared for internal distribution will be placed in a sealed envelope and marked confidential.

B. Electronic Distribution

Each employee and contractor performing work for the municipality will comply with the following policies:

1. Internally, identifying information may be transmitted using approved City's e-mail.

2. Any identifying information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail: "*This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."*

C. Access to CSD Information

1. Access to customer accounts will be job specific and approval is on a "need to know" basis. CIS access is only granted following review and joint approval by the Glendale Water & Power Information Systems Administrator and the Customer Services Administrator.

2. Employees with access to the CIS and other personal customer information are required to sign a confidentiality – security agreement.

3. Access to customer accounts shall be password protected and shall be user client specific and shall be limited to authorized personnel.

4. Such password(s) shall be controlled and validated through the city's Active Directory network access protocol.

5. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Privacy Officer and the password changed immediately.

6. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Privacy Officer.

D. Credit Card and Banking Account Numbers

1. In the event that credit card payments made over the telephone or Internet are processed through a third party service provider, such third party transactions shall be made under a valid SSL Certificate. (The SSL protocol is used for encryption of data transmissions.)

2. All customer payments made over the city's website shall be conducted by Secure HTTP. (Secure communication between web client "customer" and city's web server.)

3. Account statements and receipts for covered accounts shall not include the credit or debit card or the bank account used for payment of the covered account.

E. Sources and Types of Red Flags

In order to identify relevant red flags, GWP considers the types of accounts that it offers and maintains, the methods it provides to open accounts, and the methods it provides to assess its accounts. GWP identifies the following red flags, in each of the listed categories:

1. Alerts from consumer reporting agencies, fraud detection agencies, or service providers.

Red Flags

a. Report of fraud or active duty alert that is included with a consumer report;
b. A notice of credit freeze in response to a request for a consumer report;
c. A notice of address discrepancy provided by a consumer reporting agency;

2. Suspicious documents.

Red Flags

a. Identification or document that appear to be altered or forged;
b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
c. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears to be forged);
d. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

3. Suspicious personal identification, such as suspicious address change.

Red Flags

a. Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. For example:

   i. The address does not match any address in the consumer report; 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, such as inconsistent date of birth;
c. Personal identifying information is the same as information shown on other applications that were found to be fraudulent;
d. Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity;
e. The SSN provided is the same as that submitted by another customer.
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 applicants or customers;
g. The applicant or 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 is not consistent with personal identifying information that is on file for the customer;

4. Unusual use of or suspicious activity relating to a covered account.

Red Flags

a. Change of address for an account followed by a request to change the account holder's name;
b. Payments stop on an otherwise consistently up-to-date account;
c. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
   i. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
d. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
   i. Nonpayment when there is no history of late or missed payments;
   ii. A material change in purchasing or spending patterns;
e. An account that has been inactive for a long period of time is used *(taking into consideration the type of account, the expected pattern of usage and other relevant factors).*

f. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
g. GWP is notified that the customer is not receiving paper account statements.
h. GWP is notified of unauthorized charges or transactions in connection with a customer's account.
i. GWP is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

5. Alert from Others

Red Flag

1. Notice to GWP 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.

F. Detecting Red Flags

1. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, GWP personnel will take the following steps to obtain and verify the identity of the person opening the account:

a. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity Social Security Number, Tax Identification Number, driver's license or other identification;

b. Verify the customer's identity by authenticating information through a consumer reporting agency or physical inspection of identification.

c. Review documentation showing the existence of a business entity

2. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, GWP personnel will take the following steps to monitor transactions with an account:

a. Verify the identification of customers if they request information regarding an account.

b. Verify the identification of customers prior to making any changes to an account such as, change of billing address.

G. Responding to Red Flags

1. **New Accounts** – When an employee responsible for opening a new covered account identifies red flags indicating possible identity theft with respect to an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile the red flags, the employee shall document the information and resolution. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall document such red flags and employee shall perform one or more of the following responses, as determined to be appropriate by the Privacy Officer:

    a. Cancel the transaction and request additional identifying information from the applicant;
    b. Deny the application for the new account;
    c. Notify law enforcement of possible identity theft; or
    d. Take other appropriate action to prevent or mitigate identity theft.

2. **Existing Accounts** – When a city employee responsible for working with existing covered accounts or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile the red flags, the employee shall document the information and resolution. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall document such red flags and employee shall perform one or more of the following responses, as determined to be appropriate by the Privacy Officer:

    a. Contact the customer;
    b. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account:
        i. change any account numbers, passwords, security codes, or other security devices that permit access to an account; or
        ii. close the account;
    c. In the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue, cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector;
    d. Notify a debt collector within 24 hours of the discovery of likely or probable identity theft relating to a customer

e. Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or
f. Take other appropriate action to prevent or mitigate identity theft.

V. Program Updates

This program will be periodically reviewed and updated to reflect changes in risks and to determine whether all aspects of the program are up to date and applicable in the current business environment. At least annually, the Program Administrator will consider GWP's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts GWP maintains and changes in GWP'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 General Manager will update the Program.

VI. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rules envision a degree of confidentiality regarding GWP's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing Identity Theft.