DAWSON PUBLIC POWER DISTRICT

300 South Washington Street
P. O. Box 777 - Lexington, Nebraska - 68850
Tel. No.- 308/324/2386 – Fax No.-308/324/2907

CUSTOMER POLICY
IDENTITY THEFT PREVENTION

I. OBJECTIVE

A. The purpose of this policy is to establish an identity theft prevention program (Identity Theft Prevention Program) which establishes and implements standards of care and procedures to enable the detection, prevention and mitigation of identity theft in connection with the District's accounts which are subject to this policy. This policy will also cover the aspects of protecting employee information to prevent identity theft.

B. To establish procedures for identifying and responding appropriately to the occurrence of risk factors called "Red Flags" in order to detect, prevent and mitigate identity theft in connection with the District's new and existing customer accounts.

C. To establish procedures for responding appropriately to the receipt of a notice of address discrepancy from a Consumer Reporting Agency.

D. To provide for staff training and periodic review and updating of the Identity Theft Prevention Program.

E. To provide for oversight, implementation and administration of the Identity Theft Prevention Program by the District's senior management.

F. To identify the proper purposes for which customer consumer reports, or credit information obtained from Consumer Reporting Agencies, may be used by the District.

II. CONTENT

A. DEFINITIONS

1. **"Consumer Report"** is defined as any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which will be used at least partly to determine the consumer's eligibility to receive and pay for services. Consumer Reports are commonly known as credit reports.

2. **"Consumer Reporting Agency"** (CRA) is defined as any person which, regularly engages in assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. For example, Equifax is a CRA.

3. **"Covered Account"** means any utility account under the care and control of Dawson PPD for the purpose of providing energy services.

4. **"Red Flags"** as used herein are patterns, practices or specific activities that taken together or alone, indicate the possible occurrence of identity theft, including the following:

   a. Alerts, notifications, or other warnings received from CRAs or other service providers, such as fraud detection services, which include:

      i. Fraud or active duty alert;
      ii. Credit freeze notice; or
      iii. Address discrepancy notice informing of a substantial difference between the address provided by the consumer and the address on file with the CRA.
      iv. Inconsistent pattern of activity based on history and pattern of activity, such as recent and significant increase in volume of inquiries, unusual number of recently established credit relationships, a material change in the use of credit or an account that was closed for cause or abuse.

   b. The presentation of suspicious documents. For example:

      i. The application or identification documents appear to be altered or forged;
      ii. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer;
      iii. The documents are inconsistent with information provided by the customer; or
      iv. The documents are inconsistent with readily accessible information on file with the District.

   c. The presentation of suspicious personal identifying information, such as when:

      i. The personal identifying information is inconsistent when compared to other information on file with the District, from the customer, or from external information sources (e.g., address discrepancies, an un-issued Social Security Number (SSN), or the date of birth does not match the corresponding SSN range).
      ii. The customer fails to provide all required personal information on an application or in response to notification that the application is incomplete.

   d. The unusual use of, or other suspicious activity related to, a Covered Account, such as:

i. With a new Covered Account, the customer fails to make the first payment or makes an initial payment but no subsequent payments.
ii. A customer with a Covered Account notifies the District that he or she is not receiving paper account statements.
iii. The District is notified of unauthorized services in connection with a customer's Covered Account.
iv.
v. Repeated returned mail even though the customer with a Covered Account continues to receive electric service.

e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts held by the District.

B. DUTIES TO DETECT, PREVENT AND MITIGATE

1. General

a. All employees that have access to information in a Covered Account shall be trained to detect, and respond to, Red Flags.

b. Means of identity verification shall include:

i. Applicant's full name
ii. Mailing address;
iii. Street address;
iv. Phone number;
v. Government-issued photo identification;
vi. Passwords (whether assigned by the District or user-defined)
vii. For an individual, date of birth;
viii. For a U.S. person, a taxpayer identification number;
ix. For a non-U.S. person, one or more of the following:
1. Taxpayer identification number; passport number and country of issuance;
2. Alien identification card number; or
3. Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

2. New Accounts

a. When opening new Covered Accounts and performing other functions regarding Covered Accounts including but not limited to address and billing changes, the

identity of the applicant or customer shall be verified to the extent reasonable and practicable under the circumstances.

i. Online applications for service are encrypted during the sending process.
ii. A district employee must verify that the social security number provided is valid by researching the number at www.ssa.gov/employer/ssnv.htm.
iii. The application for service shall be scanned into the customer electronic file and then shredded.
iv. No Covered Account information shall be sent electronically unless encrypted.

b. The District should not open a new Covered Account if there is a fraud or active duty alert for the applicant or customer unless the District gathers additional information sufficient to form a reasonable belief that the user knows the identity of the applicant or customer making the request.

c. If one or more Red Flags are detected during the application process for a Covered Account, while servicing a Covered Account, or otherwise, the staff member shall notify their supervisor or the Finance Manager or Manager of Consumer and Business Services or other designated staff.

3. Existing Accounts

a. When servicing existing Covered Accounts, such as processing change of address requests, staff shall authenticate the identity of the customer as well as verify the change of address or other information on the account.

b. The District should not open a new Covered Account or make material changes to an existing Covered Account if there is a fraud or active duty alert for the applicant or customer unless the District gathers additional information sufficient to form a reasonable belief that the user knows the identity of the applicant or customer making the request.

c. If one or more Red Flags are detected while servicing a Covered Account, or otherwise, the staff member shall notify their supervisor, Finance Manager or Consumer & Business Services Manager or other designated staff.

d. The District will flag or mark Covered Accounts that are to be monitored so that any reviewer (*e.g.* Customer Service Representative, hereinafter "CSR") servicing the account can be aware of the previous Red Flags or other concerns.

4. Supervisor Actions

a. Employees who are notified of a Red Flag shall evaluate the degree of risk posed by the particular Red Flag(s).

b. In determining an appropriate response, any aggravating factors, such as additional known Red Flags increasing the risk of identity theft should be considered.

c. Appropriate responses to a Red Flag may include the following:

i. Monitoring the Covered Account for evidence of identity theft;
   A. The District will mark accounts in such a manner so as to make it known to the CSR or other employee reviewing this account of any previous Red Flag concerns.
ii. Contacting the customer;
iii. Changing any passwords, security codes, or other security devices that permit access to the Covered Account;
iv. Reopening the Covered Account with a new account number;
v. Not opening a new Covered Account;
vi. Closing an existing Covered Account;
vii. Not attempting to collect on a Covered Account or not referring a Covered Account to a debt collector;
viii. Notifying law enforcement; or
ix. Determining that no response is warranted under the particular circumstances.

5. Record Management

a. The District shall maintain records of the information used to verify the applicant's identity, including name, address and other identifying information as applicable and used by the District to identify a person's identity. These records will be retained electronically and shall be protected by a firewall and password protected access to the server. All possible paper documents should be shredded except for those documents considered legally binding contracts which would not be recognized electronically by a court of law.

b. If a governmental agency provides the District with a list of known or suspected terrorists, the District shall consult such list to determine whether the applicant appears on such list.

6. Prevention Measures

a. Employees are responsible for securing any customer information so that access to it while away from your work station will not compromise the Covered Account's right to privacy.

b. All Covered Account records should be stored and handled electronically when possible. If electronic record is printed, it shall be shredded when it is no longer needed.

c. Laptop computers should limit holding Covered Account information to the extent possible. Laptops taken on business trips shall remain with the employee at all times unless locked in a room. Laptops will NOT be placed in baggage handling.

i. All district laptop computers containing Covered Account information shall have a file program that will allow deletion of records in a manner that cannot be recovered by computer hackers.

d. Linemen using portable digital devices that carry Covered Account information should have these devices password protected using no less than 5 characters, creating an alpha and numeric composition.

e. Employees with access to other employee's files, including social security numbers, will handle said information with care and will not electronically transmit this information. Files containing this information will be held in a secure place, including electronically.

C. SERVICE PROVIDERS

1. If the District engages a service provider to perform an activity in connection with one or more Covered Accounts, the District shall take steps to ensure that such activity is conducted according to reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

2. Where appropriate, the District shall require by contract that service providers have policies and procedures to detect relevant Red Flags that may arise during performance of the services, and to either report the occurrence of the Red Flags to the District or to take appropriate steps to prevent or mitigate identity theft.

D. CONSUMER REPORTS

1. Use of Consumer Reports. Consumer Reports shall be used only in connection with the extension of credit, the extension of or provision of services to a customer, to review an account to determine if the customer meets the terms of the account and for such other legitimate corporate purposes as may be approved by corporate senior management.

2. Notice of Adverse Actions. If the District takes an adverse action based on a Consumer Report, then the District shall provide written notice either via U.S. Mail or electronic notice (*e.g.* email) to the applicant, which shall include notice of the adverse action; the name, address and toll-free telephone number of the CRA that provided such report; a

statement that the CRA did not make the decision to take adverse action and is unable to provide the consumer with specific reasons why the action was taken; and notice of the consumer's right to obtain a free copy of such report from the CRA within 60 days and to dispute the accuracy or completeness of such report, as required by applicable federal Consumer Credit Protection laws (15 U.S.C.A. §§ 1681m and 1681j).

3. Notice of Address Discrepancy

a. If the District receives a notice of address discrepancy from a CRA, the District must reasonably confirm the identity and address of the applicant.
b. The employee receiving the notice of address discrepancy shall report the notice to their supervisor or other designated staff.
c. Employees who are notified of the notice of address discrepancy shall take reasonable steps to verify the identity of the applicant by verifying the information provided by the CRA with the consumer or comparing other information maintained by the co-op about the consumer (*e.g.*, change of address notification, account records, service application, etc.).
d. If the District obtains adequate confirmation to form a reasonable belief that the applicant is the same person listed in the notice of address discrepancy (Consumer Report), then the District shall document how it resolved the address discrepancy and may proceed to open the account or to take the requested action.
e. If the District is unable to form such a reasonable belief regarding the identity of the applicant, then the District shall respond appropriately under the circumstances, such as not opening an account for the applicant, closing an existing account, or taking other actions as determined appropriate based on the circumstances.

E. FURNISHING INFORMATION

1. When furnishing information to a CRA, the District shall: report accurate information; correct and update incomplete or inaccurate information; report accounts closed voluntarily by the consumer; and report delinquent accounts that have been placed for collection, charged to profit or loss or subject to a similar action.

2. The District shall not furnish information to a CRA if the furnisher has reasonable cause to believe such information is inaccurate.

F. UPDATE AND COMPLIANCE REPORTS

1. The Identity Theft Prevention Program and the defined Red Flags should be reviewed and updated periodically based upon the following:

a. Experiences of the District with identity theft;

b. Changes in methods of identity theft;
c. Changes in methods to detect, prevent, and mitigate identity theft;
d. Changes in the types of accounts that the District offers or maintains; and
e. Changes in the District's business arrangements which would impact the Identity Theft Prevention Program, such as service provider arrangements.

2. Staff responsible for implementation of the Identity Theft Prevention Program shall provide compliance reports at least annually to the General Manager or other senior management official regarding the District's compliance with applicable law.

3. The General Manager or other senior management official shall review the compliance reports and take appropriate action, if required.

4. Compliance reports should address material matters related to the Identity Theft Prevention Program and evaluate issues such as:

a. The effectiveness of the District's policies and procedures;
b. Service provider arrangements;
c. Significant incidents involving identity theft and management's response; and
d. Recommendations for material changes to the Identity Theft Prevention Program.

G. SOCIAL SECURITY NUMBERS

1. The District shall not require customers to transmit a Social Security Number via the Internet unless the transmission is secure or encrypted.

2. The District may require a Social Security Number to establish or terminate an account, to contract for services, or to confirm the accuracy of a Social Security Number on file.

3. The District may use Social Security Numbers for internal administrative or verification purposes.

III. RESPONSIBILITY

A. The General Manager or other senior management official shall be responsible for implementation, administration and review of the Identity Theft Prevention Program.

B. The General Manager or other senior management official may suggest changes to the Identity Theft Prevention Program and guidelines, as necessary to address changing identity theft risks, for the Board's review and consideration.

C. The General Manager or other senior management official may assign the specific responsibility of implementation to members of the staff of the District.

D. The Manager of Finance and Administration or other senior management official shall oversee applicable service provider arrangements and staff training as necessary to facilitate effective implementation and oversight of service providers.