McCLOUD COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Identity Theft Prevention Program**
POLICY NUMBER: **1150**
ADOPTED: **June 22, 2009**
REVIEWED: **January 9, 2014, 8/10/23**
REVISED:

1150.10 Purpose**:** To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the program in compliance with the Federal Trade Commission's Red Flags Rule (Part 681 of Title 16 of the Code of Federal Regulations) implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

1150.20 Under the Red Flag Rule, every financial institution and creditor (including 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:

1150.21 Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program.

1150.22 Detect red flags that have been incorporated into the program.

1150.23 Identity theft.

.

1150.24 Ensure the program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft.

1150.30 Definitions:

1150.31 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: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer Internet Protocol address, or routing code.

1150.32 Identify theft means fraud committed or attempted using the identifying information of another person without authority.

1150.33 A covered account means 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. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings account.

1150.34 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.

1150.35 A red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

1150.40 Identification of Red Flags: The McCloud Community Services District identifies the following red flags, in each of the listed categories:

1150.41 Suspicious documents

1150.411 Identification document or card that appears to be forged, altered or inauthentic.

1150.412 Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.

1150.413 Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged).

1150.414 Application for service that appears to have been altered or forged.

1150.42 Suspicious Personal Identifying Information

1150.421 Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates).

1150.422 Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a credit report).

1150.423 Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.

1150.424 Identifying information presented that is consistent with fraudulent activities (example: an invalid phone number or fictitious billing address).

1150.425 Social security number presented that is the same as that of another person.

1150.426 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).

1150.427 A person's identifying information is not consistent with the information that is on file for the customer.

1150.43 Suspicious Account Activity or Unusual Use of Account

1150.431 Change of address for an account followed by a request to change the account holder's name.

1150.432 Payment stop on an otherwise consistently up-to-date account.

1150.433 Account used in a way that is not consistent with prior use (example: very high activity).

1150.434 Mail sent to the account holder repeatedly returned as undeliverable.

1150.435 Notice to the District that a customer is not receiving mail sent by the District.

1150.436 Notice to the District that an account has unauthorized activity.

1150.437 Breach in the District's computer system security.

1150.438 Unauthorized access to or use of customer account information.

1150.44 Alerts from Others

1150.441 Notice to the District 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.

1150.50 Detecting Red Flags

1150.51 New Accounts: To detect any of the red flags identified above associated with the opening of a new account, District personnel will take the following steps to obtain and verify the identity of the person opening the account.

1150.511 Require certain identifying information such as name, residential or business address, principal place of business for an entity, driver's license, contact information or other identification.

1150.512 Verify the customer's identity (example: review a driver's license or other identification card).

1150.513 Review documentation showing the existence of a business entity.

1150.514 Independently contact the customer.

1150.52 Existing Accounts: In order to detect any of the red flags identified above for an existing account, District personnel will take the following steps to monitor transactions with an account:

1150.521 Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email).

1150.522 Verify the validity of requests to change billing addresses.

1150.523 Verify changes in banking information given for billing and payment purposes.

1150.60 Preventing and Mitigating Identity Theft. In the event District 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:

1150.61 Prevent and Mitigate

1150.611 Continue to monitor an account for evidence of identity theft.

1150.612 Contact the customer.

1150.613 Change any passwords or other security devices that permit access to accounts.

1150.614 Not open a new account.

1150.615 Close an existing account.

1150.616 Reopen an account with a new number.

1150.617 Notify the Program Manager for determination of the appropriate step(s) to take.

1150.618 Notify law enforcement.

1150.619 Determine that no response is warranted under the particular circumstances.

1150.62 Protect customer identifying information

1150.621 Ensure that the District website, if there is a website, is secure or provide clear notice that the website is not secure.

1150.622 Ensure complete and secure destruction of paper documents and computer files containing customer information.

1150.623 Ensure that office computers are password protected and that computer screens lock at appropriate times.

1150.624 Keep offices clear of papers containing customer information.

1150.625 Request only the last 4 digits of social security numbers. Note: Utility billing account practices do not require social security numbers.

1150.626 Ensure computer virus protection is up to date.

1150.627 Require and keep only the kinds of customer information necessary for utility purposes.

1150.70 Program Updates: This program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the District from identity theft. The Program Manager will consider the District's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the District maintains and changes in the District's business arrangements with other entities. After considering these factors, the Program Manager will determine whether changes to the program, including the list of red flags, are warranted. If warranted, the Program Manager, through the General Manager, will present the Board of Directors with his/her recommended changes and the Board of Directors will make a determination of whether to accept, modify or reject those changes to the program.

1150.80 Program Administration: The General Manager or his/her designee will serve as Program Manager.

1150.81 Oversight: Responsibility for developing, implementing and updating this program lies with the Program Manager. The Program Manager will be responsible for program administration, for ensuring appropriate training of District staff, 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.

1150.82 Staff Training and Reports: District staff responsible for implementing the program shall be trained either by or under the direction of the Program Manager in the detection of red flags, and the responsive steps to be taken when a red flag is detected. District staff is required to report to the Program Manager on incidents of alleged identity theft, the District's compliance with the program and the effectiveness of the program.

1150.83 Specific Elements and Confidentiality. For the effectiveness of identity theft prevention programs, the red flag rule envisions a degree of confidentiality regarding the District'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 Program Manager and those employees who need to know them for purposes of preventing 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 are listed in this document.

1150.90 Authority and Revisions: This policy shall be reviewed at least biennially by the Program Manager and updated as appropriate.