VERMONT ELECTRIC COOPERATIVE, INC.
MANAGEMENT POLICY – RED FLAGS

POLICY:	Red Flags Policy		
PURPOSE:	To put in place a program to detect, prevent, and mitigate identity theft in connection with members' accounts.		
APPROVED BY:	Chief Executive Officer	**DATE APPROVED:**	10/15/2008
		DATE REVISED OR REVIEWED W/O CHANGE:	05/19/2011; 07/23/14
REVIEW BY BOARD OF DIRECTORS REQUIRED?	Yes	**DATE REVIEWED:**	

A. Policy Statement

The Red Flags Rule was first issued in 2007, and subsequently amended in 2013, to implement section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The Rules requires covered businesses to develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.

It is the policy of VEC to implement the procedures set forth below to ensure that members' confidential financial information is handled in a way that protects VEC members from identity theft.

B. Types of Covered Accounts - In identifying potential "red flags" for identify theft risks, VEC has consider the risk factors posed by the following transactions which occur between members and VEC:

1. Payments for Utility Services Rendered. Payments from members for services rendered are due within thirty (30) days of billing. VEC does not regularly provide credit to its members beyond this revolving, monthly account for utility service. Such service is rendered at a fixed physical location known to VEC. As a result, there is a low risk of misuse of identifying information to perpetrate fraud on the cooperative for utility services rendered. However, identifying information maintained by VEC could be used

to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

2. Payments for Line Extensions. Line extensions are constructed at a fixed physical location known to VEC; as a result, there is a low risk of misuse of identifying information to perpetrate fraud on the cooperative for line extensions that are paid for. However, identifying information maintained by VEC could be used to perpetrate Identity Theft and defraud other businesses in if the information was wrongfully altered or disclosed.
3. Utility Deposits. For some new members, utility deposits are required prior to the initiation of service. These amounts are held under the terms and conditions of utility's tariff, and may eventually be refunded to the member. There is some risk that a member who is a victim of Identity Theft could have the member's utility deposit refunded to an identity thief. Additionally, identifying information maintained by VEC could be used to perpetrate Identity Theft and defraud other businesses in if the information was wrongfully altered or disclosed.
4. Capital Credit Accounts. All members are eligible for allocation of capital credits in accordance with VEC's Bylaws and Board policies. Capital credits are retired in accordance with the Bylaws and Board policies, either in the form of a check to the member or a credit on the member's bill. There is some risk that a member who is a victim of Identity Theft could have the member's capital credit retirement check sent to an identity thief. Additionally, identifying information maintained by VEC could be used to perpetrate Identity Theft and defraud other businesses in if the information was wrongfully altered or disclosed.

C. Protecting Member Financial Information

1. Transactions
   - **a.** Any and all member financial information will be handled by VEC's Member Service Area or Engineering Coordinators. After hours, any financial transactions will be directed to a Member Service employee or the VEC Control Center.
   - **b.** Any notes or papers containing member personal financial information shall be destroyed (shredded) after the information has been added or changed to the member account. All information shall remain in the physical control of member services. When an employee leaves his or her work area, all personal financial information shall be removed and destroyed.
   - **c.** Only Member Service, Engineering Coordinators, and key finance personnel are authorized to access member financial information and/or member personal profiles. The employees will be authorized by their manager using the Employee Access Request form which is reviewed and approved by the VEC Information

Technology Manager. The Information Technology Manager shall update a "Current Rights Matrix" which shall be used to assign user rights within the VEC information system and the Human Resources area will maintain the matrix.

2. Methods for Opening Accounts.
   a. Obtaining Information. VEC requires that prospective members who wish to receive utility service provide information for membership with the following information: (1) name and date of birth of adult household members on the account; (2) address location where service shall be provided; (3) contact and billing information; and (4) Social Security Number or Tax Identification Number. Alternatively, if members are not comfortable with providing the Social Security Number or Tax Identification, they can provide a driver's license number and birth date.
   b. Verifying Authenticity. VEC will employ a credit reporting service to verify member information. These services provide historical identity fraud information. VEC is only using the service to identify potential identity theft. Should a red flag be identified, VEC will refer to section 6 of this policy. If no threat is identified, VEC will destroy the credit reporting information.
3. Methods for Accessing Account financial information or personal profile changes. VEC allows members to access and modify personal and financial profile information related to their accounts using the following methods:
   a. In person at VEC offices with a picture identification;
   b. Over the telephone after providing VEC's Member Service Representative with certain identifying information, such as the caller's date of birth and/or the address and telephone number of the service location and the last four digits of the member's Social Security Number or Tax Identification Number. Alternatively, if members are not comfortable with providing the Social Security Number or Tax Identification number, they can provide a driver's license number and birth date.
   c. Over the Internet using a secure password.
4. Training. All employees will receive Red Flag Policy Communication. Member Service, Engineering Coordinators, as well as identified employees will receive certification training. Refresher training will occur annually.
5. Procedures. A procedure will be maintained by the member service manager. This procedure will identify the steps required to;
   a. Open an account
   b. Make Payments
   c. Modify personal profile information

D. Previous Experience with Identity Theft. VEC is not aware of any security breach of, or unauthorized access to, its systems that are used to store members' identifying information.

VEC believes that part of the reason for this historical absence of identity theft of its members' information is due to (1) the limited services and credit provided to its members, both of which are tied to an immovable physical location; (2) the small size of most member utility deposits and capital credit retirement checks; (3) the small size of the population VEC serves; (4) the relatively low rate of change in membership; and (5) the utility's policies for securing members' personal information.

E. Detecting Identity Theft. The Member Service area will be responsible for maintaining diligence to identity theft during all financial transactions. This diligence shall include relevant red flags from the following categories as appropriate:

- **a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services, including:**
  - (1) A fraud or active duty alert is included in a consumer report;
  - (2) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;
  - (3) A consumer reporting agency provides a notice of address discrepancy;
  - (4) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member, such as:
    - (a) A recent and significant increase in the volume of inquiries;
    - (b) An unusual number of recently established credit relationships;
    - (c) A material change in the use of credit, especially with respect to recently established credit relationships; or
    - (d) An account that was closed for cause or identified for abuse of account privileges.
- **b. The presentation of suspicious documents.** Member Service Representatives and other personnel of VEC shall report to management when it appears that account documents have been altered or forged when compared to other documents in a member's file. It shall also be brought to a supervisor's attention immediately if any member presents an invalid identification, or identification that appears forged for the purpose of obtaining access to account information. Presentation of suspicious documents includes:
  - (1) Documents provided for identification that appears 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 member presenting the identification;
  - (3) Other information on the identification is not consistent with information provided by the person opening a new account or member presenting the identification;

(4) Other information on the identification is not consistent with readily accessible information that is on file with VEC, such as a membership application card; or
(5) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

c. The presentation of suspicious personal identifying information. The presentation of suspicious personal identifying information, such as a suspicious address change, can be a red flag for identity theft. VEC shall provide members access to their account information in person at the utility's offices only after verifying the member's identity through photo identification. Access to member account information via telephone or internet shall require the member to verify his or her identity using information that would only be known to the member as reflected in the member's account. Member Service Representatives shall be trained to make note in a member's file when there is a lack of correlation between information provided by a member and information contained in a file for the purposes of gaining access to account information. VEC is not to provide account information without first clearing any discrepancies in the information provided. Presentation of suspicious personal identifying information occurs when:

(1) The address on an application is the same as the address provided on a fraudulent application;
(2) The phone number on an application is the same as the number provided on a fraudulent application;
(3) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by VEC. For example:
    (a) The address on an application is fictitious, a mail drop, or a prison;
    (b) The phone number is invalid, or is associated with a pager or answering service;
    (c) The Social Security Number provided is the same as that submitted by other persons opening an account or other members;
    (d) 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 members;
    (e) The person opening the covered account or the member fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete; or
    (f) Personal identifying information provided is not consistent with personal identifying information that is on file with VEC.

d. **The unusual use of, or other suspicious activity related to, a covered account.** Member Service Representatives shall be trained to note unusual use of accounts, or suspicious activities related to accounts and verify the identity of members in such circumstances. It shall further be the policy of VEC to not provide identifying information to members, either verbally or in writing, even when members are asking for their own information. Member Service Representatives shall immediately notify management, who will conduct further reasonable inquiry, when a member requests such information. It shall be the policy of VEC to train its Member Service representatives to look for unusual activity when reviewing member accounts for service. Member Service Representatives shall also notify a supervisor when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the member. For requests for cooperative membership lists for use in cooperative elections, VEC shall take steps to ensure that the requested information is only disclosed in accordance with its Member Request for Cooperative Corporate Information policy. Suspicious activities include:
   (1) Shortly following the notice of a change of address for a member account, VEC receives a request for the addition of authorized users on the account;
   (2) Mail sent to the member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member's covered account;
   (3) VEC is notified that the member is not receiving paper account statements;
   (4) VEC is notified of unauthorized charges or transactions in connection with the member's account;
   (5) A member requests a capital credit check or utility deposit refund check be sent to a new address without requesting a service disconnection or change in service location;
   (6) A member requests that a capital credit check or utility deposit refund check be made payable to a person other than the member; or
   (7) A member requests that VEC provide the member with personal identifying information from the cooperative's records.

e. **Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.** Upon notice from a member, law enforcement authority, or other persons that one of its members may be a victim of identity theft, VEC shall contact the member directly in order to determine what steps may be necessary to protect any member information in the possession of VEC. Such steps may include, but not be limited to, setting up a new account for the member with additional identifying

information that may be identified only by the member in order to protect the integrity of the member's account, or notifying members and the media of an on-going attempt to perpetrate a fraud on the membership. Such notices include:

(1) Notice from members, law enforcement authorities, or other persons indicating that a member has been a victim of Identity Theft;

(2) Notice to the cooperative that a member has provided information to someone fraudulently claiming to represent the cooperative;

(3) Notice to the cooperative that a fraudulent website that appears similar to the cooperative's website is being used to solicit member personal identifying information;

(4) The cooperative's mail servers are receiving returned e-mails that the cooperative did not send, indicating that is member may have received a fraudulent e-mail soliciting member personal identifying information.

f. VEC does not generally receive consumer reports related to its members. For this reason, VEC does not anticipate receiving any consumer reports that might alert it to potential Identity Theft related to a member. However, if VEC does receive such a report, Member Service Representatives shall report such activity to supervisors for further review and inquiry.

F. Responses to Potential Identify Theft

All suspicions shall be directed to the Member Service Manager. The Member Service Manager shall respond appropriately to detect red flags to prevent and mitigate any possible identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

a. Monitor a covered account for evidence of identity theft;

b. Contact the member;

c. Change any passwords, security codes or other security devices that permit access to a covered account;

d. Reopen a covered account with a new account number;

e. Not open a new covered account;

f. Close an existing covered account;

g. Notify law enforcement; or

h. Determine no response is warranted under the particular circumstances.

G. Assuring Data Security

1. VEC is restricting access to their computer systems by:

a. External access to the network is restricted by two-factor authentication and VPN.

b. Data containing member's personal information is stored only on iVUE system.

c. Only current employees of VEC have access to iVUE.

d. Access to personal information (such as SSN) is limited only to member's service department. Members services manager authorizes security change in order to grant VEC employees access to that type of information.

e. Attempt to login with incorrect password cause to suspend account on iVUE (prevention against unauthorized access).

f. Tapes with data backups are handled only by designated IT personnel.

2. Vendors and Service Providers (Third Party Compliance)
   (1) Those Vendors and/or Service Providers that interact with members and are handling personal financial information will be required to submit a statement verifying that the company complies with the Red Flag Rule.
   (2) Those Vendors and/or Service Providers that store data with member's personal financial information will be required to state what policies and/or national standards that the organization complies with to ensure the information is secure.
   (3) Records of Security Statements from Vendors and Service providers shall be maintained by the VEC Corporate Services Department in accordance with the VEC Records Retention Procedure.

H. Administration of this Policy

1. VEC shall consider updates at least annually to determine whether it has experienced any Identity Theft of its members' accounts, whether changes in the methods of identity theft require updates to this policy, and whether changes are necessary to detect, prevent, and mitigate identity theft. VEC's management will continue to monitor changes in methods of identity theft, and re-evaluate this policy in light of those changes. Management believes that review of such changes on no more than an annual basis is necessary. Administration of this Policy shall be as follows:
   a. The Board of Directors has adopted this policy and will have ultimate authority over this policy, but the policy shall be managed by the Chief Executive Officer (CEO) of VEC. The CEO shall have authority to delegate oversight and compliance to other individuals at the senior level management level. The CEO shall be responsible for reviewing staff and management reports regarding compliance with the utility's policy.
   b. Potential changes to the policy shall be reviewed at least annually by VEC management. Material changes to the policy that may be needed prior to the meeting described herein shall be brought to the CEO's attention, and reviewed by management and the Board of Directors if deemed necessary by the CEO.

c. All employees will be advised of their Red Flag responsibilities annually. Specified VEC employees will receive Red Flag refresher training annually.

d. Reports.

(1) Management personnel assigned responsibility under this policy or by delegation from the CEO shall prepare a report, at least annually, regarding the implementation and progress of the utility's policy for review by the CEO. The CEO may, at his or her discretion, bring any issues related to the policy to the attention of the Board of Directors for review.

(2) The above-described report prepared by management personnel designated with supervising the policy shall include a discussion of: the progress of implementing and the effectiveness of the policy; ongoing risk level of Identity Theft of member information; potential changes to the policy and other operation practices of the utility to further the goal of protecting member's personal information; and, identification and discussion of instances of Identity Theft of the utility's members.

(3) The CEO shall keep records of meeting regarding this policy showing the dates and topics discussed.

e. Outside Audits. VEC will conduct an outside Red Flag conformance audit of at least once every three years