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 Cooperative's accounts which are subject to this policy.

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 Cooperative's new and existing customer accounts that are used primarily for personal purposes or by a sole proprietor for primarily personal purposes.

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 Cooperative'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 Cooperative.

G. To provide for the creation and maintenance of an Identity Theft Compliance Manual to be used by employees of Jefferson Energy Cooperative in handling and addressing Red Flags as may be required.

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 a utility account primarily for personal, family or household purposes and a utility account primarily for a sole proprietor's small business purposes where there is a reasonably foreseeable risk to the sole proprietor of identity theft.

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 (although Jefferson Energy Cooperative shall not be required to affirmatively seek notice of such alerts);
        ii. Credit freeze notice (although Jefferson Energy Cooperative shall not be required to affirmatively seek notice of such 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 Cooperative.

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 Cooperative, 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.
   iii. The personal identifying information is of a type commonly associated with fraudulent activity, such as invalid phone number, mail drop or prison address, provided that Jefferson Energy Cooperative shall not be required to affirmatively seek to uncover this type of Red Flag.

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 Cooperative that he or she is not receiving paper account statements. iii. The Cooperative is notified of unauthorized services in connection with a customer's Covered Account. iv. A Covered Account is used in a manner that is inconsistent with established patterns of activity on the account (e.g. non typical activity in bill payment).

v. A Covered Account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

vi. 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 Cooperative.

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. Employees shall be provided with a copy of the Jefferson Energy Cooperative Identity Theft Compliance Manual. The purpose of the manual will be to establish the procedures to be followed by employees when handling certain types of information and certain Red Flags.

b. Means of identity verification may 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 Cooperative or user- to provide authentication of request)
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.

b. The Cooperative should not open a new Covered Account if there is a fraud or active duty alert for the applicant or customer unless the Cooperative 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 Jefferson Energy's Director of Loss Control and Compliance 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 Cooperative 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 Cooperative 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 or Jefferson Energy's Director of Loss Control and Prevention or other designated staff.

d. The Cooperative will flag or mark Covered Accounts that are to be monitored so that any reviewer (*e.g*. Member Service Representative, hereinafter "MSR") 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 Cooperative will mark accounts in such a manner so as to make it known to the MSR 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 Cooperative 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 Cooperative to identify a person's identity.

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

C. SERVICE PROVIDERS

1. If the Cooperative engages a service provider to perform an activity in connection with one or more Covered Accounts, the Cooperative 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 Cooperative 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 Cooperative 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 Cooperative takes an adverse action such as denial of service based on a Consumer Report, then the Cooperative **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 Cooperative receives a notice of address discrepancy from a CRA, the Cooperative 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 Jefferson Energy's Director of Loss Control and Prevention.
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 Cooperative 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 Cooperative shall document how it resolved the address discrepancy and may proceed to open the account or to take the requested action.
e. If the Cooperative is unable to form such a reasonable belief regarding the identity of the applicant, then the Cooperative 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 Cooperative 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 Cooperative 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 Cooperative 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 Cooperative offers or maintains; and
   e. Changes in the Cooperative'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 CEO, General Manager or other senior management official regarding the Cooperative's compliance with applicable law.

3. The CEO 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 Cooperative'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.

III. RESPONSIBILITY

A. The CEO shall be responsible for implementation, administration and review of the Identity Theft Prevention Program.

B. The CEO 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 CEO may assign the specific responsibility of implementation to members of the staff of the Cooperative. Specifically, the CEO is authorized to designate an Identity Theft Prevention Committee to be comprised of select Managers and employees. The Committee shall provide updates to the CEO on a periodic basis and shall be charged with updating the Identity Theft Prevention Compliance Manual.

D. The Vice President of Energy Services shall oversee applicable service provider arrangements and staff training as necessary to facilitate effective implementation and oversight of service providers.

ADOPTED: March 25, 2009

Acknowledgement of Receipt / Review
of
Policy 125 – Identity Theft Prevention

JEC holds employees responsible for our privacy principles. Each JEC employee is personally responsible for maintaining consumer confidence in the company. We provide training and communications programs designed to educate employees about the meaning and requirements of Identity Theft Prevention. We conduct internal audits and commission outside-expert reviews of our compliance with the privacy principles and the specific policies and practices that support the principles. Employees who violate these principles or other company policies and practices are subject to disciplinary action, up to and including dismissal. Employees are expected to report violations -- and may do so confidentially -- to their managers or Director of Loss Control and Compliance.

JEC uses information security safeguards. Access to customer data is limited to those who specifically need it to conduct their business responsibilities. We use security techniques designed to protect our customer data -- especially when certain data is used by employees and business partners to fulfill customer services.

JEC limits the release of customer information. We release information only with the members' consent or request, or when required to do so by law or other regulatory authority. When a court order or subpoena requires release of information, we notify the customer promptly to give the customer an opportunity to exercise his or her legal rights. The only exceptions to this policy are when we are prohibited by court order or law from notifying the customer, or cases in which fraud and/or criminal activity is suspected.

JEC ensures information quality. We use advanced technology and well-defined employee practices to help ensure that customer data is processed promptly, accurately and completely. We require high standards of quality from the consumer reporting agencies and others who provide us with information about prospective members.

JEC is responsive to members' requests for explanations. If we deny an application for our services or end a customer's relationship with us, to the extent permitted by applicable laws, we provide an explanation, if requested. We state the reasons for the action taken and the information upon which the decision was based, unless the issue involves potential criminal activity.

JEC extends these privacy principles to its business relationships. We expect the companies we select as our business partners to honor our privacy principles in the handling of customer information. These include companies that assist us in providing services to our members or supply us with information for identifying or evaluating prospective members.

I HAVE RECEIVED AND REVIEWED A COPY OF THE JEC POLICY 125 – IDENTITY THEFT PREVENTION. I ACKNOWLEDGE THAT IT IS MY RESPONSIBILITY TO HOLD MEMBER INFORMATION IN THE UTMOST CONFIDENCE, AND I WILL NOT MISUSE MEMBER DATA DURING OR AFTER MY TERM OF EMPLOYMENT WITH JEC.

_____	_____	_____
Employee Signature	Employee Name (Print)	Date