POLICY NO. 303

IDENTITY THEFT RED FLAG PREVENTION
MEMBER INFORMATION PRIVACY

I. OBJECTIVE

It shall be the policy of Inter-County Energy Cooperative Corporation ("Inter-County Energy") to take all reasonable steps to identify, detect and prevent the theft of its members' personal information – commonly known as Identity Theft. In order to carry out that policy, Inter-County Energy hereby adopts the following policy for identifying and detecting Red Flags that should raise concerns for Inter-County Energy that a member's information is potentially being misused or stolen.

Individual privacy is very important, therefore, Inter-County Energy will only collect and use information needed to offer and fulfill its core business purposes. Inter-County Energy will be lawful and fair to the individual whose data it is storing and will retain only what is needed to maintain its relationship with the individual. This means Inter-County Energy will not disclose information for an unrelated purpose without the consent of the individual or by authority of law. Inter-County Energy's ability to successfully implement its business is dependent on maintaining accurate information, therefore, Inter-County Energy will strive to keep information it holds concerning customers accurate. Inter-County Energy will be open about how it uses data, will not trade or sell an individual's personal data and will not use cookies. For more information about Inter-County Energy's privacy protection practices contact the President/CEO.

Inter-County Energy respects the privacy and confidentiality of member information and is committed to operational practices that protect member information. This policy describes the information that Inter-County Energy as a utility, collects from its members as a routine part of its operations, and how it uses, protects and shares the information it collects.

II. DEFINITIONS

Member – Person, firm, corporation or body politic applying for or receiving service from Inter-County Energy.

Red Flag – A pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Identity Theft – A fraud committed or attempted using the identifying information of another person without authority.

Privacy – Non-disclosure of member information to an unassociated third-party without member consent.

Member Personal Identifying Information – Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, Social Security Number, date of birth, official state or government

issued driver's license or identification number, alien registration number, government passport number, employer or address.

Member Operational Information – Member information that does not identify an individual member but includes detailed data about system operations about utility services or programs provided to a member.

Anonymous Member Information – Information of more than one member combined in such a manner that does not identify a member.

Utility – Inter-County Energy and third-party contractors, vendors or other agents with whom it is necessary to share member information to provide energy services and energy efficiency programs provided by Inter-County Energy. For direct payments or rebates made to the members by an associated third-party, a controlled set of member PERSONAL IDENTIFYING INFORMATION is provided to the vendor.

Associated Third-Party – Includes contractors, vendors, energy efficiency program partners, governmental entities or agents and non-profit utility-assistance organizations with which Inter-County Energy interacts.

Unassociated Third-Party – Any person or entity not directly involved with the routine operations of the utility.

III. POLICY RATIONALE

Under federal law and regulations, Inter-County Energy is required to adopt and implement an Identity Theft Red Flag Prevention Policy no later than the compliance deadline of November 1, 2008. This is required under the Federal Trade Commission ("FTC") regulations at 16 C.F.R. § 681.2 *et seq.*

IV. IDENTIFICATION OF ACCOUNTS SUBJECT TO RED FLAG POLICY

Inter-County Energy maintains accounts for its members that allow the members to pay for service after it has been rendered. Bills are sent and payments are due on a monthly basis. These accounts are covered by this Red Flag policy.

V. IDENTIFICATION OF POTENTIAL RED FLAGS

A. Risk Factors

In identifying potential Red Flags associated with the accounts that Inter-County Energy maintains, Inter-County Energy's Board of Directors and Management have considered the following Identity Theft risk factors:

1. Types of Covered Accounts - Inter-County Energy is an electric cooperative serving rural and small towns in Kentucky, providing its members with electric utility service. Inter-County Energy serves approximately 25,600 members. Payments from members for services rendered are due within fifteen (15) days of billing. Inter-County Energy does not provide credit to its

members beyond the normal course of business. Such service is rendered at a fixed physical location known to Inter-County Energy.

2. Methods for Opening Accounts - Inter-County Energy requires that prospective members who wish to receive utility service submit a membership application with the following information:

   (a) name and date of birth of adult household members on the account;

   (b) address location where service shall be provided;

   (c) contact and billing information; and

   (d) Social Security Number or Driver's License number.

   The applicant must also present to the Customer Service Representative a valid Government issued photo identification as proof of identity.

3. Methods for Accessing Accounts - Inter-County Energy allows members to access information related to their accounts using the following methods, or plans to allow such access in the near future:

   (a) in person at Inter-County Energy's offices with a picture identification;

   (b) over the telephone after providing Inter-County Energy Customer Service Representative with certain Personal 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; or

   (c) over the Internet using a secure password.

4. Previous Experience with Identity Theft - Inter-County Energy is not aware of any security breach of or unauthorized access to its systems that are used to store members' Personal Identifying Information. Given the limited amount and types of services and credit provided to its members, the small size of the population it serves, and the relatively low rate of change in membership, coupled with the utility's policies for securing members' personal information, Inter-County Energy believes the risk of its members being the subject of Identity Theft through the information collected by Inter-County Energy to be low.

B. Sources of Red Flags

In identifying potential Red Flags associated with the accounts that Inter-County Energy maintains, Inter-County Energy's Board of Directors and Management have considered the following sources of Red Flags for Identity Theft:

1. Past Incidents of Identity Theft - Inter-County Energy is not aware of any security breach of or unauthorized access to its systems that are used to store

members' Personal Identifying Information collected by the utility. In the event of incidents of Identity Theft in the future, such incidents shall be used to identify additional Red Flags and added to this policy.

2. Identified Changes in Identity Theft Risk - As provided in Section VIII below, Inter-County Energy will at least annually review this policy, the utility's operations and the utility's experience with Identity Theft for changes in Identity Theft risk.

3. Applicable Supervisory Guidance - In addition to considering the guidelines initially published with the FTC's Red Flag regulations, as a part of its annual review, Inter-County Energy will review additional regulatory guidance from the FTC and other consumer protection authorities.

C. Categories of Red Flags

In identifying potential Red Flags associated with the accounts that Inter-County Energy maintains, Inter-County Energy's Board of Directors and Management have considered the following categories of Red Flags for Identity Theft:

1. Alerts, Notifications, and Warnings - Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services, can be Red Flags for Identity Theft. Such alerts, notifications and warnings include:

   (a) A fraud or active duty alert is included in a consumer report.

   (b) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

   (c) A consumer reporting agency provides a notice of address discrepancy.

   (d) 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:

      1) A recent and significant increase in the volume of inquiries;

      2) An unusual number of recently established credit relationships;

      3) A material change in the use of credit, especially with respect to recently established credit relationships; or

      4) An account that was closed for cause or identified for abuse of account privileges.

   Required Response:

   Inter-County Energy will receive and utilize reports related to its members from a consumer reporting agency. For the purpose of this policy, alerts,

notifications and warnings received from such reports shall be considered to be a Red Flag.

2. Suspicious Documents - The presentation of suspicious documents can be a Red Flag for Identity Theft. Suspicious documents include:

   (a) Documents provided for identification that appears to have been altered or forged.

   (b) The photograph or physical description on the identification is not consistent with the appearance of the applicant or member presenting the identification.

   (c) Other information on the identification is not consistent with information provided by the person opening a new account or member presenting the identification.

   (d) Other information on the identification is not consistent with readily accessible information that is on file with Inter-County Energy, such as a membership application form.

   (e) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

   Required Response:

   Customer Service Representatives and other personnel of Inter-County Energy 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 Management's attention immediately if any member presents an invalid identification, or identification that appears forged for the purpose of obtaining access to account information.

3. 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. Presentation of suspicious information occurs when:

   (a) Personal Identifying Information provided is inconsistent when compared against external information sources used by Inter-County Energy. For example:

      1) The address does not match any address in the consumer report; or

      2) The Social Security Number has not been issued, or there is an indication that the Social Security Number belongs to a deceased person.

(b) Personal Identifying Information provided by the member is not consistent with other personal identifying information provided by the member. For example, there is a lack of correlation between the Social Security Number range and date of birth.

(c) Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by Inter-County Energy, for example:

1) The address on an application is the same as the address provided on a fraudulent application; or

2) The phone number on an application is the same as the number provided on a fraudulent application.

(d) Personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Inter-County Energy. For example:

1) The address on an application is fictitious, a mail drop, or a prison; or

2) The phone number is invalid, or is associated with a pager or answering service.

(e) The Social Security Number provided is the same as that submitted by other persons opening an account or other members.

(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 other persons opening accounts or other members.

(g) 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.

(h) Personal Identifying Information provided is not consistent with personal identifying information that is on file with Inter-County Energy Cooperative Corporation.

(i) If Inter-County Energy uses challenge questions, the person opening the account or the member cannot provide authenticating information beyond that which generally would be available from a wallet.

Required Response:

Inter-County Energy 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.

Customer 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. Inter-County Energy is not to provide account information without first clearing any discrepancies in the information provided.

4. Suspicious Activity - The unusual use of, or other suspicious activity related to, a member account is also a Red Flag for potential Identity Theft. Suspicious activities include:

   (a) Shortly following the notice of a change of address for a member account, Inter-County Energy receives a request for the addition of authorized users on the account.

   (b) Mail sent to the member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member's covered account.

   (c) Inter-County Energy is notified that the member is not receiving paper account statements.

   (d) Inter-County Energy is notified of unauthorized charges or transactions in connection with the member's account.

   Required Response:

   Customer Service Representatives shall be trained to note unusual use of accounts, or suspicious activities related to accounts. It shall further be the policy of Inter-County Energy to never provide Social Security Numbers or Tax Identification Numbers to members, either verbally or in writing, even where a member is asking for their own information. Customer Service Representatives shall immediately notify Management, who will conduct further reasonable inquiry, when a member requests such information.

   It shall be the policy of Inter-County Energy to train its Customer Service Representatives to look for unusual activity when reviewing member accounts for service. Customer Service Representatives shall also notify Management 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.

5. Notices - Notice from members, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with member accounts can also be a Red Flag for Identity Theft.

   Required Response:

Upon notice from a member, law enforcement authority, or other persons that one of its members may be a victim of Identity Theft, Inter-County Energy shall contact the member directly in order to determine what steps may be necessary to protect any member information in the possession of Inter-County Energy. 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.

VI. DETECTING RED FLAGS

A. It shall be the policy of Inter-County Energy to obtain Personal Identifying Information about, and verify the identity of, a person opening an account. Inter-County Energy Corporation will obtain the member's name, date of birth, address for service location and Social Security Number or Tax Identification Number to open a new account.

It shall be the policy of Inter-County Energy to never provide Social Security Numbers or Tax Identification Numbers to members, either verbally or in writing, even where a member is asking for their own information.

B. It shall be the policy of Inter-County Energy to authenticate members and customers, monitor transactions and verify the validity of change of address requests, in the case of existing accounts.

VII. PREVENTING AND MITIGATING IDENTITY THEFT

A. If Inter-County Energy discovers that any of its members have become a victim of Identity Theft through personal information used by the utility in opening or maintaining a member's account, Management shall take appropriate steps that it deems necessary to mitigate the impacts of such Identity Theft. These steps may include, but are not limited to:

1. Monitoring an account for evidence of Identity Theft;

2. Contacting the member;

3. Changing any passwords, security codes or other security devices that permit access to an account;

4. Reopening an account with a new account number;

5. Closing an existing account;

6. Not attempting to collect on an account;

7. Notifying the member;

8. Notifying law enforcement; or

9. Determining that no response is warranted under the particular circumstances.

VIII. ACCOUNTABILITY

A. Inter-County Energy assumes the following:

1. It is accountable for the member's Personal Identifying Information within the organization's possession or control.

2. Inter-County Energy will use contractual or other means to provide a comparable level of protection for personal information that has been transferred to an associated third party for processing.

3. It will not sell the Personal Identifying Information of its members.

4. It will not collect information indiscriminately and will limit collection of information to that which is reasonable and necessary to provide electric service, participation in an energy efficiency program, use of a specific tariff or other program.

5. It will adopt procedures to protect personal information in its control, to receive and respond to complaints and inquiries and train employees regarding these policies and procedures.

B. Member Information Collected

Personal and operational information obtained by Inter-County Energy for a member and associated persons on the member's account include, but aren't limited, to the following:

1. The name and address and other contact information, such as telephone numbers, e-mail address;

2. Facts regarding consumption of energy, both historic and current;

3. Data concerning a member's transactions with Inter-County Energy, such as account numbers, account balances, payment history;

4. Credit and reference information, such as date of birth, social security number, employment information, driver's license, previous addresses, and general financial data;

5. Medical information to be used in case of emergency power outages; and

6. Financial institution information for pre-authorized payments.

C. Purposes of Member Information Collected

Inter-County Energy obtains personal and/or operational member information for the following purposes to:

1. Personalize, identify, communicate and conduct the business of Inter-County Energy;

2. Verify or establish the existence of a member's energy service;

3. Assess credit risk, including obtaining credit reports;

4. Communicate with the member and address any service issues or needs;

5. Bill accounts, maintain payment records, give notice on current balance;

6. Assemble statistics about how Inter-County Energy's website is accessed and used;

7. Compile aggregate data that does not identify the member as an individual;

8. Contact members about outages and services offered by Inter-County Energy and third-party energy-efficiency programs partners;

9. Provide aggregated information to Community Action Council ("CAC") agencies, upon request;

10. Respond to federal, state, local regulatory agencies; and

11. Collect debts owed by a member

D. Member Access to Information

Members shall have access to their individual information, including but not limited to, historical data regarding electric usage, respective billing units and the current applicable tariff by the following methods:

1. The internet member portal may be accessed by all Inter-County Energy members by using a personal User ID and Password through Inter-County Energy's website at: www.intercountyenergy.net. If a personal security code has not been established, the member may contact Inter-County Energy by telephone and assistance will be provided on how to set up the code.

2. Members may contact Inter-County Energy and the requested information will be mailed directly to the member or may be picked up by the member, with proper identification, at one of Inter-County Energy's offices during regular business hours.

E. Disclosure of Member List

A member list may be requested pursuant to *BOARD POLICY 420, MEMBER REQUESTS FOR COOPERATIVE INFORMATION.*

F. Security

1. Inter-County Energy maintains member information with reasonable and appropriate technical, administrative, physical and cyber safeguards to protect against loss, unauthorized access, destruction, misuse, modification, and improper disclosure of member-consumer information.

2. A summary of this Identity Theft Red Flag Prevention/Member Information Privacy Policy will be posted on the Inter-County Energy website.

G. How to Contact Inter-County Energy

This policy is maintained by Inter-County Energy at the headquarters office located below. Questions regarding the policy may be directed to this office.

Inter-County Energy Cooperative
Attn: Member Privacy
1009 Hustonville Road
Danville, KY 40422
E-mail at: mail@intercountyenergy.net
Telephone: 859-236-4561 or 1-888-266-7322

IX. UPDATING AND ADMINISTERING THE POLICY

A. Inter-County Energy Cooperative Corporation 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 updating to this Policy, or whether changes are necessary to detect, prevent, and mitigate Identity Theft. Inter-County Energy Cooperative Corporation'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.

B. Administration of the Policy shall be as follows:

1. The Board of Directors has adopted this Policy and will have ultimate oversight of this Policy, but the Policy shall be managed by the President/CEO of Inter-County Energy Cooperative Corporation. The President/CEO shall establish a Privacy Committee to create, drive and monitor the program. The President/CEO shall appoint a Privacy Officer who will function as the head of the committee. He/she shall be from Senior Management and shall report directly to the President/CEO regarding the outcomes and needs of the Identity Theft Prevention Program. The President/CEO shall be responsible for reviewing Privacy Committee and Management reports regarding compliance with the utility's Policy.

2. Potential changes to the Policy shall be reviewed at least annually at a meeting of the utility's Privacy Committee. The purpose of this meeting will be to evaluate incidents involving Identity Theft and Management's response and recommendations for changes in the program. Material changes to the Policy that may be needed prior to the meeting described herein shall be brought to the attention of the Privacy Officer and the President/CEO, and reviewed by Management and the Board of Directors if deemed necessary by the President/CEO.

3. Reports

(a) Management reports shall be prepared at least annually by the Privacy Committee regarding the implementation and progress of the utility's Policy for review by the President/CEO. The President/CEO may, at his or her discretion, bring any issues related to the Policy to the attention of the Board of Directors for review.

(b) The above-described report prepared by the Privacy Committee 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.

(c) The President/CEO shall keep records of meetings regarding this Policy showing the dates and topics discussed. The President/CEO shall also cause to be maintained a file with copies of the five (5) most recent annual reports prepared under the policy.

Effective: October 17, 2008
Revised: October 8, 2010
Reviewed: October 21, 2011
Reviewed: October 19, 2012
Revised: October 18, 2013
Revised: July 18, 2014
Reviewed: July 24, 2015
Revised: May 16, 2016
Reviewed: July 15, 2016
Reviewed: July 21, 2017
Reviewed: July 20, 2018
Revised: July 26, 2019