PURPOSE:

To offer guidelines that the Cooperative and Board of Directors shall follow while adhering to the procedures of an identity theft prevention program.

POLICY:

It is the policy of this Cooperative to identify and mitigate possible identity theft and fraud through the use of internal procedures and financial Red Flags. The cooperative will take steps to detect Red Flags indicating possible identity theft, prevent identity theft, and mitigate any identity theft activities or security breaches. Oakdale Electric Cooperative recognizes the responsibility to safeguard personal customer information within the workplace. The purpose of this policy is to create an Identity Theft Prevention Program utilizing guides set forth in the FACT Act (2003) and Federal Register Volume 72, Number 217, Friday November 9, 2007.

Red flags are defined as “patterns, practices, or specific activities that indicate the possible existence of identity theft”. These red flags may include use of personal identifying information (Wis Stats 943.201(b)) and sensitive information such as;

- Complete or partial names
- Initials
- Birthdates
- Social security number or taxpayer ID number
- Address
- Telephone number, mobile phone number or pager number
- Drivers license number
- Individuals place of employment or employee number
- Maiden name of mother
- Number of depository account
- Credit information
- Account numbers
- Financial/member account numbers
- Personal identification codes or means of account access
- Individuals deoxyribonucleic acid profile or biometric data
- Other personally related information or personal identification data

PROCEDURES:

A. It is the goal of the Cooperative to identify the pattern, practice or specific activity that indicates the existence of identity theft.
B. The Cooperative will take actions to mitigate and correct any activity that results in or would result in identity theft.
C. It is the Cooperative’s policy to protect its member’s, employee’s and Director’s identity and sensitive information.
D. Employees will be informed of, and trained to recognize, red flags indicating the possible identity theft.

E. The Cooperative will establish a Privacy Committee consisting of persons from Management, the IT section, member services, financial, and human resources.
    (1) The Privacy committee will review and develop red flags indicating possible identity theft or fraud.
    (2) This committee will complete a needs assessment
    (3) The privacy committee will perform quarterly review of red flags reported and acted upon by employees.
    (4) The Privacy committee will report findings, red flag activities and areas of possible improvement to the General Manager.
    (5) The Privacy Committee will perform periodic risk assessments to determine what improvements to mitigate
    (6) The Privacy Committee will facilitate periodic training of employees about this policy and its updates.

F. Red Flags include but are not limited to:
    1. Fraud Alert from Credit agencies
    2. Name and social security number do not match, or name is inaccurately spelled.
    3. Credit reports show inconsistencies
    4. A consumer fraud alert or active duty alert
    5. Any account that would adversely affect a consumer's credit standing should be considered at risk of identity theft and thus subject to a red flag
    6. An address discrepancy reported by a consumer reporting agency
    7. A consumer's communication with the financial institution or creditor about attempted or actual identity theft should always be a red flag
    8. A company's knowledge of a security breach within its own confines or that of an affiliate with which the company has shared customer data
    9. Attempts to open a new account with altered documents
    10. Suspicious actions by employees such as downloading customer account information or being added to a customer account
    11. Notice that the consumer's information may have been lost or stolen through a data security breach
    12. An address discrepancy on a credit application sent by a consumer in response to a company's solicitation generated by credit report prescreening or other marketing lists
    13. Alerts distributed by government, trade associations, or media reports about recent trends in identity theft
    14. A creditor or financial institution learns that its business identity has been fraudulently used to obtain personal information, such as in phishing schemes
    15. The presentation of suspicious documents
    16. The presentation of suspicious person identifying information, such as suspicious address change;
    17. The unusual use of, or other suspicious activity related to a member account,
    18. Notice from members, victims of identity theft; law enforcement authorities or other persons regarding possible identity theft in connection with member accounts held by the Cooperative
    19. Notice from the member or others that a credit or debit card has been lost or stolen
    20. Activity in a dormant account

G. Needs Assessment
    1. The privacy committee will perform needs assessment looking in the following two areas: 1. new accounts and 2. existing account transactions. The

committee will look at existing practices to determine strengths and weaknesses and determine areas of improvement.

2. The privacy committee will promote and facilitate the **detection** of red flags, the methods needed to **prevent** identity theft, and facilitate **mitigation** once identity theft or security breach has occurred.

H. Opening a new account

1. Applicants for electrical services will provide documentation that will identify them. Government issued identification will accepted for identification such as a State issued drivers license, certified birth certificate or passport. Customer service representatives will cross-reference data provided by the applicant with data provided by a credit reporting agency such as Online Utility Exchange. If discrepancies exist, a determination will have to be made by Senior Management on what actions are to be taken.
2. If the identity of the applicant cannot be confirmed through identification papers and a credit reporting agency, the County Detective responsible for financial crimes may have to be notified as directed by Senior Management.
3. The privacy Committee will compile and report findings and actions taken periodically to the General Manager.

I. Monitoring Existing Accounts

1. If payments are made in a fashion that raises a Red Flag, Senior management shall be notified and action shall be taken to determine when identity theft or identity fraud has taken place.
2. If Identity theft or fraud has taken place, Senior management will determine who gets notified including the victim and the County Financial Crimes Detective, and how they are notified. Other actions to be taken will be determined by Senior Management to mitigate the possible losses sustained.
3. If identity theft occurs, the victim should notify the Cooperative in writing, with a copy of the complete FTC affidavit and police report.
4. The Privacy Committee will compile and report findings and actions taken periodically to the General Manager.

J. Information Technology Assessments

1. IT persons will periodically (at least annually) assess risks of identity theft through our computer systems, computers and data bases and report the results to the Privacy Committee.
2. If a breach in security of the computer system occurs, Senior management will be immediately notified.
3. Actions will be taken to mitigate the breach and possible loss of personal data and determine what accounts or what members might be affected.
4. Senior Management will determine when and how a member is notified that their personal information may be compromised.
5. Senior Management will determine when a county financial crimes Detective is notified.

K. Red Flag Working Procedure

1. The Privacy Committee will develop and maintain a working procedure manual for detecting, preventing, and mitigating Red Flag events and identity theft.
2. This Manual will be kept current by the Privacy Officer

3. Employees will be periodically trained how to identify Red Flags.

L. Medical Confidentiality
   1. The Cooperative shall not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility unless it is part of protocol for a particular service. All medical information will be treated as confidential and rules of protection against identity theft apply as to all other private information.

M. Periodically, internal staff may review practices to ensure compliance with corporate policy. The reports will be used to evaluate effectiveness of and amend the Identity Theft Program. External auditors may review the program. An Annual report reviewing all incidents, program revisions, and goals will be submitted by the General Manager to the Board of Directors.

N. Training and Orientation
Employees that deal with personal identifying information will be trained once using a workbook developed by the privacy committee. These employees will be updated periodically as the Red Flag procedures change. Other employees will be trained to recognize red flags and about identity theft in general. The workbook will include case studies, discussion of red flags, procedures to document red flags including notifications, references, and forms, and mitigation consistent with this policy. New employees and employees newly assigned to jobs involving personal identifying information will be trained using the above referenced workbook. Management will be trained using a management level workbook developed by the Privacy Committee. This training will include a discussion of mitigation of red flag events and security breaches.

O. Contractors will be held to the same standard when dealing with information relating to Cooperative employees or members. Terms and conditions will require contractors to detect identity theft, prevent identity theft through proactive action, and mitigate any identity theft or security breach, and notify the cooperative about such activities in a timely fashion.

P. The General Manager & CEO is responsible for assuring this policy is implemented.

Issued:	**Reviewed Date (no revisions):**	**Revised Date:**
10-29-2008	**08-27-2019, 7-29-2020, 2-23-2022, 03-02-2023, 02-29-2024, 03-03-2025**	