SULLIVAN COUNTY RURAL ELECTRIC COOPERATIVE, INC.
FORKSVILLE, PA

Board Policy No. 603

SUBJECT: Identity Theft Prevention Program

I. PURPOSE

To detect the possibility of identity theft, protect the identity and financial data of our members, and comply with the requirements of the FTC and the "Red Flags" Rule.

II. CONTENT

A. The Chief Executive Officer will be responsible for ongoing involvement in oversight, development, implementation and administration of the Identity Theft Prevention Program.

B. Training for employees will be provided as necessary by the Chief Executive Officer or Manager, Finance & Administration.

C. An annual report will be made and presented to the Board of Directors on compliance with the program and any significant incidents experienced for the year. The report will include:

1. The effectiveness of the policies and procedures in addressing the risk of identity theft.

2. Significant incidents that have occurred and management's response.

3. Recommendations for changing the program.

D. As risk factors are discovered, such as identity theft, member information breach, etc., the policy will be revised to address any future risks.

E. An investigation will be conducted by the Manager, Finance & Administration when any of the following "Red Flags" are discovered:

1. Incidents of identity theft.

2. Fraud alerts, active duty alert, credit freezes, address discrepancies, invalid Social Security number, notifications, or other warnings received from a consumer-reporting agency or service provider.

3. The presentation of suspicious documents, such as altered or forged memberships or right-of-ways.

4. The presentation of suspicious personal identification information (Name, Social Security #, address, telephone number, etc.) that differs from what the person is telling you or that doesn't match with other information such as a signature on a document or a check.

5. The unusual use of an account such as nonpayment when there is no history of missed payments, a major shift in usage patterns or mail that is returned or complaints of not receiving bills.

6. Notice from members, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.

F. When signing up a new member or changing an address for an existing member, effort should be made to verify the information given especially if there are any suspicious circumstances. If deemed necessary by the staff, the member will be required to come into the office to prove identification.

G. To protect the identity and financial data of our members, their Social Security number is only on the membership form which is scanned and shredded. Only selected office personnel have access to this information.

H. Monitoring the security of member identity data must be an ongoing process. When a member's information has been jeopardized, the following procedure should be followed.

1. Contact the member.

2. Eliminate the breach of information.

3. If appropriate, notify law enforcement.

I. The Chief Executive Officer and Manager, Finance & Administration will provide ongoing oversight of third party software providers and service providers that utilize member information to ensure the member identity information is secure and utilized properly.

III. RESPONSIBILITY

The Chief Executive Officer is responsible for the administration of this policy.

IV. This policy supersedes and cancels all other policies which relate to the subject matter herein and which may be in conflict herewith.

Date adopted:	October 16, 2008	Attest:	Walter E. Botsford, Secretary
Revised:	April 16, 2009		Walter E. Botsford, Secretary
	February 18, 2010		Walter E. Botsford, Secretary
	February 16, 2012		Walter E. Botsford, Secretary
	February 6, 2014		Walter E. Botsford, Secretary
	February 20,2020		Kathy A. Robbins, Secretary
	April 15, 2021		

Kathy A. Robbins, Secretary