WELLS RURAL ELECTRIC COMPANY
Adopted: October 8, 2009 Revised:
Reviewed:

POLICY NO. 2 - 10

IDENTITY THEFT PROTECTION

I. OBJECTIVES

A. This policy is developed to ensure privacy and accuracy of consumer credit report information, and to reduce incidence of identity theft and aid victims.

B. To protect employees, members, customers, contractors and the company from damages related to loss or misuse of sensitive information.

C. This policy applies to employees, contractors, consultants, temporaries, and other workers at the company, including all personnel affiliated with third parties.

II. POLICY

A. Identify Red Flags

Red Flags are a pattern, practice, or specific activity that indicates the possible existence of identity theft. Red Flags shall be identified utilizing the following methods:

1. Alerts, Notifications or Warnings from a Consumer Reporting Agency
2. Suspicious Documents
3. Suspicious Personal Identifying Information
4. Unusual Use of, or Suspicious Activity Related to, an Account
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft

B. Detect Red Flags

Detecting Red Flags shall be accomplished by system and transaction monitoring, and the receipt of reports, warnings, alerts, etc. from the appropriate entities.

C. Response to Red Flags

The appropriate response to a Red Flag that has been detected needs to be commensurate with the degree of risk posed. Aggravating factors should be considered that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records, or notice that a customer has provided information related to an account to someone fraudulently claiming to represent Wells Rural Electric Company or to a fraudulent website. Appropriate responses are indicated in the Identity Theft Prevention Program.

D. Updates to the Program

Annual evaluation and adjustment of the Identity Theft Prevention Program in light of the results of testing and ongoing monitoring of the program, material changes to the company's operations or business arrangements or "any other" circumstances that may have a material impact on the effectiveness of the security program shall be accomplished.

III. RESPONSIBILITY

It will be the responsibility of the Chief Executive Officer and his staff to enforce this policy and the Identity Theft Prevention Program to ensure that it is followed by employees and contractors.

The Chief Executive Officer will assure that the Identity Theft Prevention Program will be updated on an annual basis, employee training accomplished, and any updates to the program supplied to the Chief Executive Officer and staff.