Beartooth Electric Cooperative, Inc.

MEMBER RELATIONS POLICY NO. 411

1. SUBJECT: IDENTITY THEFT PREVENTION PROGRAM

2. OBJECTIVE: To protect the identity/financial data of our member owners and minimize the possibility of identity theft of member information, and to comply with the requirements of the Federal Trade Commission (FTC) and the "Red Flags" Rule.

3. POLICY:

3.1. The finance personnel will be responsible for ongoing involvement in oversight, development, implementation and administration of the Identity Theft Prevention Program.

3.2. Training for the employees will be provided as necessary.

3.3. Oversight of third party software providers will ensure that they also comply with the program.

3.4. An annual report will be made by the auditor and presented to the Board on compliance with the program and any incidents experienced for the year. The report will include:

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

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

3.4.3. Recommendations for changing the program.

3.5. As risk factors are discovered, such as identity theft or member information breach, the policy will be revised to address any reasonably foreseeable risks.

3.6. An investigation will be conducted when any of the following "Red Flags" are discovered:

3.6.1. Incidents of identity theft.

3.6.2. Methods of identity theft that reflect changes in identity theft risks.

3.6.3. Alerts, notifications or other warnings received from a consumer reporting agency or service provider.

3.6.4. The presentation of suspicious documents, such as altered or forged.

3.6.5. The presentation of suspicious personal identification information.

3.6.6. The unusual use of an account.

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

3.6.8. A fraud alert is included with a consumer report.

3.6.9. A consumer-reporting agency provides a notice of address discrepancy.

3.6.10. Identification photo that does not match the person.

3.6.11. Invalid social security number.

3.6.12. The unusual use of or other suspicious activity related to a covered account.

3.7. When signing up a new member or changing an address for an existing member, reasonable care will be exercised to verify the information given.

3.8. Monitoring the security of member identity data is an ongoing process. When a member's information has been jeopardized, the following procedure will be followed:

3.8.1. Contact the member.

3.8.2. Eliminate the breach of information.

3.8.3. If appropriate, notify law enforcement.

3.9. The finance personnel will review the activity of third party software providers and service providers that utilize member information with the intent that the member identity information is reasonably secure and utilized properly.

4. RESPONSIBILITY:

The General Manager shall ensure that the provisions of this policy are followed.

Adopted: 11/25/2014
Revised: 3/28/2017
Reference: LV417
Review Date: March 2019

Attest: /s/ David Peterson
Board President

Attest: /s/ Julie Lindgren
Secretary/Treasurer