SULLIVAN COUNTY RURAL ELECTRIC COOPERATIVE, INC.
FORKSVILLE, PA

Board Policy No. 604

SUBJECT: Merchant Security Policy

I. PURPOSE

To establish policy for secure handling of sensitive card holder data including but not limited to magnetic strip data, Primary Account Numbers (PAN's), expiration date, and service code. To detail the requirements for safeguarding Cooperative's cardholder data for Payment Card Industry (PCI) compliance.

II. CONTENT

A. Protecting and Managing Cardholder Data

Protecting cardholder data is paramount. Allowing data theft or destruction, inadvertently sharing confidential information, infecting system networks with viruses, misusing Cooperative resources, allowing theft of Cooperative property and allowing compromise of private or confidential Cooperative or client information are examples of what might result from a security compromise.

1. All sending of unencrypted Primary Account Numbers by end-user messaging technologies (i.e., email, instant messaging, and chat) are strictly prohibited.

2. Access to system components and cardholder data is limited to only those authorized individuals whose job require such access or have a need-to-know. This authority is granted by the CEO and Manager, Finance and Administration and reviewed annually.

3. All paper that contains cardholder data is to be identified and physically secured in a locked drawer. No electronic cardholder data will ever be stored.

4. Strict control to be maintained over internal or external distribution of any kind of media that contains cardholder data:

    a. Media is classified and clearly marked as confidential.
    b. If necessary media is sent by secured courier or other delivery method that can be accurately tracked.

5. Chief Executive Officer or Manager, Finance and Administration approval is required prior to moving any and all media containing cardholder data from a secured area.

6. Strict control must be maintained over storage and accessibility of media that contains cardholder data.

7. Media containing cardholder data is to be destroyed when it is no longer needed for business or legal reasons:

    a. Paper materials are to be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
    b. The general rule is that media containing cardholder date will be destroyed when over 180 days old. Exceptions to the rule must be approved by Chief Executive Officer or Manager, Finance and Administration.

8. All computers in the PCI environment must run an anti-virus product. This product must be capable of detecting, removing and protecting against malicious software. This product must have automatic updates and periodic scans enabled. Anti-virus logs are generated and retained at least one year with the last three months immediately available.

9. Any website used for processing credit cards must use Secure Socket Layer (SSL) encryption . The website must not accept or ask for credit card information unless https:// is present and lock icon is locked.

10. All system components and software in the PCI environment must have the latest vendor supplied patches. Critical security patches must be applied within 30 days of release.

B. Policy Maintenance and Employee/Contractor Awareness

1. Review of this policy will be conducted on an annual basis or as changes to the environment occurs.

2. Usage of employee-facing technologies such as remote access, wireless, electronic media, internet, PDA's and wireless will adhere to the following:

    a. No unauthorized equipment can be brought in or set up in the Cooperative's facility. This includes, but is not limited to modems, computers or wireless devices.

b. Wireless devices must be set up securely by establishing secure accounts/passwords, disabling SSID broadcasts and using the highest available encryption for the device.

3. Manager, Finance and Administration is designated with security responsibility.

4. These security policies will be formally reviewed annually with all employees.

5. A list of Service Providers must be maintained. This list will be updated and reviewed by Manager, Finance and Administration when necessary but at least annually.

6. A written Agreement is required from each Service Provider including an acknowledgement that they are responsible for the security of cardholder data they posses.

7. Due diligence is to be performed prior to the engagement of Service Providers. Procedures performed will include when possible:

   a. A visit to the Service Providers physical offices to discuss security practices and procedure with their management and staff.
   b. A written statement acknowledging their responsibilities to securely process, handle and transmit cardholder data.
   c. Written proof that the Service Provider is PCI compliant.
   d. Request reliable industry references.

8. A program is to be maintained to monitor Service Providers' PCI DSS compliance status. On an annual basis a request for a new compliance certificate will be requested.

III. RESPONSIBILITY

It shall be the responsibility of the Chief Executive Officer to administer this policy.

IV.

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

Date adopted: February 6, 2014 Attest:

Walter E. Botsford, Secretary