

# **INFORMATION SECURITY PLAN FOR SOUTH CENTRAL INDIANA REMC**

## **I. INTRODUCTION**

In order to serve its members, South Central Indiana REMC (“SCI REMC”) will acquire and maintain data and information, to provide financing for member energy conservation projects. In order to protect the information which is acquired and maintained by SCI REMC and to comply with Federal Law, specifically The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley Act (“GLBA”), 15 U.S.C. § 6801, SCI REMC will have an Information Security Plan (“Plan”).<sup>1</sup> The GLBA requires that SCI REMC appoint an Information Security Plan Coordinator to assess the risk of likely security breaches, institute a training program for all employees who have access to covered data and information, oversee service providers and evaluate and adjust the Plan periodically.

## **II. COMPLIANCE MEASURES**

### **A. The Coordinator**

In order to comply with GLBA, SCI REMC has designated the Director of Information Services (“Coordinator”) to coordinate the Plan. All correspondence and inquiries with regard to the Plan should be directed to the Coordinator.

The Coordinator will assist in identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information which could result in the compromise of such information. The Coordinator will also evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program; and regularly monitor and evaluate the program.

### **B. Relevant Areas**

Relevant areas to be considered when assessing the risks to customer information include:

- Customer Services and Marketing
- Affected Information Systems / Information Technology Services
- Service Providers

---

<sup>1</sup> For the purposes of this Plan, **covered data and information** includes, but is not limited to customer financial information required to be protected under the GLBA. **Customer financial information** is that information which SCI REMC has obtained from a customer in the process of offering a financial product or service, or such information provided to SCI REMC by another financial institution. Offering a financial product or service includes offering financing for energy conservation projects. Examples of customer financial information includes addresses, telephone numbers, bank and credit card account numbers, income and credit histories, and social security numbers, in both paper and electronic format.

For SCI REMC, the Customer Services and Marketing Department will handle and maintain customer information. SCI REMC recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of covered data and information through third parties

SCI REMC recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Coordinator will actively communicate internally regarding identification of new risks.

### **C. Evaluating the Effectiveness of the Current Safeguards in Place**

Current safeguards taken to protect customer information include the following:

#### **Description**

- Computer access limited by system ID's and passwords
- Staff has only limited access to paper reports in file cabinets
- Building is locked after hours
- Data is backed up nightly
- Passwords that expire periodically and employees must then reset them
- Passwords not posted in publicly viewable places
- Antivirus protection maintained on computer systems
- Firewalls installed on computer systems
- Separation of customer information from recycling and shredding of those records
- Referring calls or other requests for customer information to designated individuals and being alert to fraudulent attempts to obtain this information
- Keeping customer information stored in appropriate filing cabinets and clear of areas with public access
- Customer information accessible only by those who "need to know"

- When providing copies of information to others, remove non-essential and personally identifiable information that has no relevance to the transaction
- Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information
- Avoid leaving computer terminals unattended when personally identifiable information is on the screen
- Position or adapt computer terminal monitors so that personally identifiable information is visible only to the authorized user of the terminal
- Reduce paper forms and documents through increased web access to this information or through internal digital imaging or document managing
- Ensure precautionary measures are taken when discussing personal or confidential information over the telephone
- Centralized files
- Off-site storage retention of critical files and documents
- Implement measures to ensure unauthorized persons cannot access computer systems when left unattended

*The effectiveness of the above safeguards is dependent upon*

- Ensuring compliance with the safeguards
- Implementation of additional safeguards as described below

#### **D. Implementing Supplemental Measures**

Additional safeguard measures that are recommended to supplement current safeguards include the following:

#### **Description**

- Lock file cabinets containing customer information and maintain a list of persons with access to the locked cabinets
- Evaluate procedures to detect the improper disclosure or theft of customer information

#### **E. Social Security Numbers**

Social security numbers are considered protected information under the GLBA. The Coordinator will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are used, and in what instances members are being asked to provide a social security number. The Coordinator will maintain a written record of this assessment to assist in continuing the evaluation and adjustment of this plan.

#### **F. Coordination of SCI REMC's Information Security Plan**

The Coordinator will implement and update the Plan. A written security policy detailing the information security policies and processes will be maintained by the division with access to the protected customer information.

### **III. SERVICE PROVIDERS**

Service Providers that are given access to covered data and information will be neither selected nor retained unless they provide adequate safeguards. Contracts with service providers shall include the following provisions:

- a specific definition of the confidential information being provided;
- a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- a guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
- a guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
- a provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- a stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
- a stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles SCI REMC to immediately terminate the contract without penalty;
- a provision which requires the service provider to defend, indemnify, and hold SCI REMC harmless for any damages resulting from violation of the contract's protective conditions;
- a provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
- a provision ensuring that the contract's protective requirements shall survive any termination of the agreement.

### **IV. EMPLOYEE TRAINING AND EDUCATION**

The Coordinator will develop training and education programs for all employees who have access to covered data. This training will include physical handling and disposition of non-electronic documents containing customer information as well as proper procedures to follow in processing storing electronic information and documents.

References of new employees working in areas that regularly work with covered data and information are checked. Each new employee is also trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including

“pretext calling”<sup>2</sup> and how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information security.

## V. PHYSICAL SECURITY

SCI REMC has addressed the physical security of covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal member information, accounts, balances and transactional information are available only to SCI REMC employees with an appropriate business need for such information.

Loan files, account information and other paper documents are kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees know combinations and/or the location of keys. Paper documents that contain covered data and information are shredded at time of disposal.

## VI. INFORMATION SYSTEMS

The Federal Trade Commission (“FTC”) defines information systems as including network and software design, and information processing, storage, transmission, retrieval and disposal. Guidelines on how to maintain security throughout the life cycle of customer information – from data entry to data disposal are as follows:

- In order to protect the security and integrity of the network and its data, the Coordinator will develop and maintain a registry of all computers attached to the network. This registry will include, where relevant, IP address or subnet, physical location, operating system, intended use (server, personal computer, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine had or has special access to any confidential data covered by relevant external laws or regulations.
- The Coordinator bears primary responsibility for the identification of internal and external risk assessment, but all members of SCI REMC are involved in risk assessment. The Coordinator will conduct periodic risk assessments, including but not limited to the categories listed by the GLBA.<sup>3</sup>

---

<sup>2</sup> “Pretext calling” occurs when an individual improperly obtains personal information of SCI REMC members so as to be able to commit identity theft. It is accomplished by contacting SCI REMC, posing as a member or someone authorized to have the member’s information, and through the use of trickery and deceit, convincing an employee of SCI REMC to release member identifying information.

<sup>3</sup> 16 C.F.R. § 314.4(b) *et. seq.*:

...

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- The Coordinator will assure the physical security of all servers and terminals which contain or have access to covered data and information.
- The Coordinator will, to the extent feasible, develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

## **VII. EVALUATION AND REVISION OF THE PLAN**

The Plan shall be evaluated and adjusted in light of relevant circumstances, including changes in SCI REMC's business arrangements or operation, or as a result of monitoring the safeguards. Periodic auditing of each relevant area's compliance and general risk assessment will be performed as determined by the Coordinator. Evaluation of the risk of new or changed business arrangements by the Coordinator will be done in consultation with the Chief Executive Officer and the Director of Customer Service and Marketing.

219660

- 
- (1) Employee training and management;
  - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
  - (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
  - (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
  - (d) Oversee service providers, by:
    - (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
    - (2) Requiring your service providers by contract to implement and maintain such safeguards.
  - (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.