SCDC POLICY

NUMBER: GA-06.12

TITLE: PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) COMPLIANCE

ISSUE DATE: JUNE 9, 2020

RESPONSIBLE AUTHORITY: DIVISION OF INFORMATION SECURITY AND PRIVACY

POLICY MANUAL: GENERAL ADMINISTRATION

SUPERSEDES: NONE - NEW POLICY

RELEVANT SCDC FORMS/SUPPLIES:

ACA/CAC STANDARDS:

STATE/FEDERAL STATUTES:

PURPOSE: This policy provides information to ensure SCDC is compliant with the Payment Card Industry Data Security Standard (PCI DSS) and informs employees what is expected of them. The purpose of the PCI DSS is to protect cardholder data, whether it is in paper or electric form, from hackers and thieves. PCI DSS involves technical and operational requirements to help prevent security breaches, card fraud, and other security vulnerabilities.

SCOPE: All SCDC employees who have access to and manage payment card terminals for business transactions. This includes full time and part time employees, contractors, volunteers, interns, and vendors. Any area of SCDC wishing to implement a card payment system must follow this policy prior to the implementation.

POLICY STATEMENT: It is always the intent of SCDC to follow all requirements of the PCI DSS. Compliance not only entails maintaining secure systems that process card payment data, establishing roles and responsibilities, implementing necessary processes and procedures, but educating appropriate employees regarding their responsibilities.

TABLE OF CONTENTS

SPECIFIC PROCEDURES:

1. ROLES AND RESPONSIBILITIES: The purpose of this section is to establish responsibilities and roles for each individual or division that processes card payments. All SCDC card payment terminals are encrypted, therefore, SCDC does not store card data.

1.1 SCDC is responsible for:

1.1.1 Requiring background checks on potential personnel who will handle payment card transactions prior to hire.

1.2 All areas accepting card payments are responsible for:

1.2.1 Designating an individual who will have primary authority and responsibility for payment acceptance.

1.2.2 Confirming the identity of any third-party person claiming to be maintenance personnel.

1.2.3 Conducting daily device checks for tampering and substitution on payment terminals.

1.2.4 Storing all payment devices that process credit cards in a locked space with limited access when not in use, including when needing replacement or repair.

1.2.5 Destroying media when it is no longer needed for SCDC business purposes.

1.2.6 Only issuing equipment pre-approved by the divisions of RIM and Information Security & Privacy to process card payments.

1.2.7 Creating and maintaining documentation of card payment devices used, including:

1.2.7.1 Make and model of device.

1.2.7.2 Location of device(s) and divisions responsible for the device.

1.2.7.3 Device serial number or other method of unique identification.

1.2.7.4 When new devices are added, relocated, and decommissioned.

1.2.8 A list of card payment devices, including make and model, location, and device serial number or other unique identification, shall be sent to the Division of Information Security & Privacy as soon as reasonable when changes are made to the list, or, if no changes are made, annually.

1.3 Where applicable, ensuring that the default security configurations, such as passwords and usernames, shall be changed before being placed into use.

1.4 Ensuring that where employee access to the terminals is required, each individual user shall have their own unique ID (e.g., username and password) for accessing the device terminals.

1.5 Creating and maintaining documentation of service providers and a written agreement that includes an acknowledgement on details of the service being provided and responsibilities of each party.

1.6 The Division of Information Security and Privacy is responsible for completing an annual self-assessment questionnaire (SAQ) and attesting to SCDC's compliance with PCI DSS.

2. SECURITY INCIDENT PLAN: The purpose of this section is to have an incident response plan implemented that prepares an immediate response to a system breach. This portion of the policy falls in compliance of the PCI DSS requirement 12.10. No part of this security incident plan shall supersede SCDC Policy GA-06.05, "IT Security," but only act as an addendum for payment card devices.

2.1 Incidents: Any unauthorized access to a system that contains confidential or restricted data is collected, processed, or transmitted is an incident.

2.2 Point of contact: In case of a suspected or confirmed incident, contact the response team by sending an email documenting the incident to: ISP@doc.sc.gov. The Division of Information Security & Privacy will immediately confirm that they are aware of the incident with a response to the initial notification.

2.2 Each SCDC workplace must take reasonable and necessary steps to assure that confidential/restricted information cannot be accessed by individuals who do not have a job-related reason for accessing that confidential/restricted information.

2.3 The Division of Information Security & Privacy shall form a Response Team which may include members of RIM and other necessary personnel (to include employees of the division using the card payment system) to handle the incident.

2.4 Once an incident is discovered or relayed to the Response Team, incident handling will be conducted according to SCDC Policy GA-06.05.

3. EMPLOYEE TRAINING: The purpose of this section is to develop a formal security awareness program for SCDC employees who utilize card payment terminals while conducting daily operations. This training must include how to verify the identity of any third-party persons claiming to be maintenance or repair personnel, be aware of suspicious behavior around devices, and reporting malicious indications of device tampering or substitution. The training shall be validated by the Division of Information Security & Privacy to meet PCI DSS requirements and conducted through the Division of Training. Third party substitutes will not be recognized unless authorized by the Division of Training with the advisement of the Division of Information Security & Privacy.

3.1 Employee Awareness Program: The supervisor or manager of all areas that use card payment devices are required to:

3.1.1 Assign training to employees prior to working with payment card terminals;

3.1.2 Have employees complete training annually for a refresher;

3.1.3 Maintain documentation of employees that completed initial and annual training; and

3.1.4 Sign PCI Security Awareness Training and Confidentiality Agreement.

4. ANNUAL POLICY REVIEW AND UPDATE: PCI DSS requires that this policy must be reviewed annually and updated by the Division of Information Security & Privacy when changes occur.

SIGNATURE ON FILE

s/Bryan P. Stirling, Director

Date of Signature

ORIGINAL SIGNED COPY MAINTAINED IN THE OFFICE OF POLICY DEVELOPMENT