THE HONORABLE CURTIS M. LOFTIS, JR.
State Treasurer

POLICY
Compliance with PCI Data Security Standard
July 1, 2016

Purpose:
To prescribe the requirement for governmental entities participating in the statewide Merchant Card Services contract to comply with the PCI Data Security Standard (PCI DSS). Compliance with the PCI DSS is a contractual obligation of each participant. Compliance with the standard serves to assist in the protection of cardholder data. Failure to comply with the standard increases the possibility of security breaches and exposes the participant to the risk of potential fines levied by the card brands.

Authority:
§ 11-5-280. *Acceptance of credit cards by state agencies.*
The State Treasurer may enter into contracts allowing a state agency or institution to accept credit cards as payment for goods or services provided.

§ 1-11-490. *Breach of security of state agency data; notification; rights and remedies of injured parties; penalties; notification of Consumer Protection Division.*

Program Administration:
The State Treasurer's Office (STO) provides eligible entities (including state agencies, universities, colleges, and local units of government) the opportunity to secure merchant card services under a statewide master services agreement, procured through the State Fiscal Accountability Authority (SFAA). Each entity subscribing to the merchant card services do so by executing an Agency Participation Agreement. The agreement obligates the entity to at all times adhere to the current version of the PCI Data Security Standard, which is promulgated by the PCI Security Council.

Each of the card brands requires the merchant card processor [i.e., SunTrust Merchant Services, LLC (STMS)] to monitor the merchants the processor serves to ensure compliance with the PCI DSS. There are three elements of compliance with the PCI DSS process:

- Compliance with the standard
- Validation of compliance with the standard
- Attestation of validation of compliance with the standard

Compliance with the PCI DSS is in accordance with the most current version of the standard promulgated by the PCI Security Council.

Validation of compliance with PCI DSS entails:

- Preparing the appropriate Self-Assessment Questionnaire (SAQ) on an annual basis (applies to all participants)
- Undergoing quarterly external vulnerability scanning of external (public) facing IP addresses, performed by an Approved Scanning Vendor (applies to card capture solutions that involve connecting to the internet).

Attestation of validation of compliance is performed when requested by either the merchant card processor (STMS) or by either one of the card brands. STMS intends to request attestation at least annually. In the event of a security breach, the card brands will be requiring proof of PCI DSS compliance at the time of the breach.

General Policy: As a prerequisite for participating in the statewide merchant card services agreement provided by the State Treasurer's Office, each participant must execute a participation agreement, which among other things, obligates the participant to comply with the PCI Data Security Standard (PCI DSS). Each participant must subscribe to the appropriate services that allows for the validation of PCI compliance.

Basic PCI Compliance Validation Services (CVS)

Each participant must subscribe to the basic PCI Compliance Validation Services (CVS) provided by a qualified security services provider:

- All participants must subscribe to a service that provides for the annual completion of the appropriate online Security Assessment Questionnaire (SAQ), as required by the PCI DSS.
- All participants that utilize one or more capture methods involving external facing IP addresses, and are subject to undergoing external vulnerability scans as required by the PCI DSS, are to subscribe to a remote external vulnerability scanning service.

Participants that are considered level 3 or level 4 merchants have two options to obtain PCI Compliance Validation Services:

- Subscribe to STMS's PCI Rapid Comply® Service (provided at no charge by STMS); or
- Contract with a qualified security services provider to perform the two required tasks

Participants that are considered level 1 or level 2 merchants must utilize a qualified security assessor (QSA) to perform their validation tasks.

Extensive PCI Related Services

Depending upon the complexity of a participant's card capture process, the participant may be required to subscribe to more extensive PCI related services. Examples of extensive services include internal vulnerability scanning, internal penetration testing, external penetration testing, compliance assessment services, and remediation services.

Such extensive services are not available through STMS's PCI Rapid Comply® Service. Therefore, the participant must procure such services through the appropriate procurement process. Any statewide or convenience contract that may be available from the Materials Management Office or Division of Information Security (DIS) should be considered.

Compliance Policies:

The following policies pertain to the ongoing PCI compliance process:

- Any costs incurred by a participant to become and remain compliant with the PCI Data Security Standard shall be borne by the participant.

- Any participant that does not subscribe to the applicable component of a basic PCI Compliance Validation Service (CVS) shall not be allowed to participate or continue to participate in the Merchant Card Services master agreement.

- Each participant subscribing to a compliance validation service shall perform all requirements of the service in a timely manner in order to reflect and attest the status of PCI compliance when and if requested by either the merchant card processor or a card brand.

- The role of the State Treasurer's Office shall be to provide general guidance regarding the requirements of the PCI Data Security Standard and to secure a service (e.g., STMS's PCI Rapid Comply® Service) through which the participant can validate its compliance with the standard.

- The role of the merchant card processor (STMS) shall be to monitor the participant's compliance status and to determine any remediation action that the processor deems appropriate. The processor may address any non-compliance issue directly with the participant.

- The participant is responsible for obtaining, from a qualified vendor, any applicable services necessary to comply with the PCI Data Security Standard, such as penetration testing, compliance assessment, qualified security assessor (QSA) support, and remediation services.

- Any participant receiving communications from the merchant card processor regarding a PCI Data Security non-compliance issue must respond to the processor within a reasonable time. Corrective actions must be taken that satisfies the processor's concerns. Actions taken may include, but not be limited to:
    - Correcting the non-compliance issue within the timeframe agreed to by the processor
    - Implementing compensating measures agreed to by the processor
    - Temporarily suspending the use of a merchant card capture application until the non-compliance issue is resolved
    - Discontinuing the merchant card capture application altogether

- The participant's "employee PCI awareness training program," as required by Section 12.6 of the standard, should address individuals who are members of both the IT staff and user staff.

- The participant's security incident plan, as required by Section 12.10 of the standard, should address the timely notification requirements specified by the card brands, as well as specified by SC Code § 1-11-490, "*Breach of security of state agency data; notification; rights and remedies of injured parties; penalties; notification of Consumer Protection Division.*" Should a security incident occur, the State Treasurer's Office, as sponsor of the master contract, should be notified, so as to ensure coordination of any required notifications to the merchant card processor (STMS).

- Prior to engagement with any third-party service provider, the participant must verify the provider's PCI compliance status and obtain a written agreement that identifies the provider's responsibilities regarding compliance roles, pursuant to Sections 12.8 and 12.9 of the standard.

- The individual (or his/her successor) at the governmental entity that executed the "Participation Agreement" to allow the entity to be a participant in the statewide merchant card services master services agreement shall be the individual responsible for ensuring that the requirements of this policy are adhered to, including but not limited to, responding to any non-compliance issues that may arise.

- This policy is intended to supplement any applicable policies and requirements of the Division of Information Security (DIS) and the South Carolina Information Security (INFOSEC) Program.

Approval of Policy Implementation

Curtis M. Loftis, Jr. South Carolina State Treasurer