OREGON STATE TREASURY

Origination:	*12/2019*
Last Approved:	*12/2019*
Last Revised:	*12/2019*
Next Review:	*12/2021*
Owner:	*Bryan González: Policy & Strategy Manager*
Policy Area:	*Finance*
References:	

FIN 215: Payment Card Industry Data Security Standard (PCI DSS) Compliance Validation Requirements

INTRODUCTION & OVERVIEW

Summary Policy Statement

Pursuant to its designation as the sole banking and cash management officer for the State of Oregon, the Oregon State Treasury ("Treasury") has broad authority to review, establish, and modify policies and procedures for the efficient and secure handling of cash and cash equivalents under the control of all Agencies. Agencies are directed to employ the principles, standards, and related requirements for cash management prescribed by Treasury. This policy establishes how Agencies will demonstrate the ability to maintain compliance with the Payment Card Industry Data Security Standards (PCI DSS) related to merchant card acceptance.

Purpose and Goals

The purpose of this policy is to require Agencies to utilize a validation service for the assessment and verification of the correct implementation of security controls, procedures, and policies as per the requirements of the PCI DSS. Failure to comply with the PCI DSS standards may result in fines, loss of ability to process payment cards, and reputational damage to Agencies and/or state government.

Applicability

The provisions of this policy apply to Agencies as defined within that participate in the merchant card acceptance program through Treasury's Master Agreement for Merchant Card Services.

Authority

ORS 293.875 and ORS 352.135(3)

POLICY PROVISIONS

Definitions

Acquirer: An entity that processes Payment Card transactions on behalf of Merchants. Elavon is the Acquirer for Agency Payment Card transactions through Treasury's Master Agreement for Merchant Card Services with U.S. Bank/Elavon.

Agency (Agencies): Every state officer, board, commission, department, institution, branch or agency of the state government, whose costs are paid wholly or in part from funds held at Treasury. While excluded, at times, in other legal contexts, includes Treasury, Secretary of State, Judicial Department, Legislative Assembly, and the Public Defense Services Commission. Agency also is used here to reference those other entities, including public universities, that hold funds at Treasury by virtue of an intergovernmental or other agreement.

Approved Scanning Vendor (ASV): An organization approved by the PCI Security Standards Council to validate adherence to the PCI DSS scan requirements by performing vulnerability scans of internet-facing environments of Merchants and service providers.

Attestation of Compliance (AOC): A form for Merchants and service providers to attest to the results of a PCI DSS assessment, as documented in a Self-Assessment Questionnaire or Report on Compliance. It is required to be made by the agency annually, and is the last step performed after completion of each applicable SAQ.

Cash Management: Generally includes, but is not limited to, the collection and deposit of, handling or management of, and payment, use, or transfer of moneys of an entity or organization.

Merchant: An entity authorized to accept Payment Cards for the payment of goods and services.

Payment Card: A general term used to describe credit, debit, and prepaid cards bearing the logos of American Express, Discover, MasterCard or Visa.

Payment Card Industry Data Security Standard (PCI DSS): The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures associated with credit and debit card account data. The standard was developed by the founding payment card brands of the PCI Security Standards Council which includes American Express, Discover, JCB International, MasterCard, and Visa. The purpose was to help to facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is intended to help organizations proactively protect customer card account data that is either accepted, transmitted, processed, or stored. All Merchants and Service Providers, regardless of the annual transaction volume, are required by the various card brands to comply with the standard.

PCI DSS Compliance: Maintaining payment security is required for all entities that store, process, or transmit cardholder data. Guidance for maintaining payment security is provided in the PCI Data Security Standards. These set the technical and operational requirements for organizations accepting or processing payment transactions and for software developers and manufacturers of applications and devices used in those transactions. There are four PCI security standards that Agencies functioning as Merchants must adhere to: (1) the PCI Data Security Standard (PCI DSS), which applies to an Agency's entire Payment Card process; (2) the Payment Application Data Security Standard (PA-DSS), which applies to the capture software that an Agency may be using; (3) the PCI Pin Transaction Security Requirements (PCI PTS), which apply to terminals and devices that provide for the keying of PIN debit cards (also referred to as PCI PIN Entry Device or PCI

PED); and, (4) PCI Point-to-Point Encryption (P2PE), which applies to point-to-point encryption solution providers that an Agency might be using.

Qualified Security Assessor (QSA): An independent security organization qualified by the PCI Security Standards Council to validate an entity's adherence to the PCI DSS. A QSA employee is an individual employed by a QSA and bears a certificate evidencing satisfaction of all QSA requirements.

Report on Compliance (ROC): A summary of evidence derived from a Qualified Security Assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROC provides a comprehensive summary of testing activities performed and information collected during the assessment against the PCI DSS Requirements and Security Assessment Procedures. The information contained in an ROC must provide enough detail and coverage to verify that the assessed entity is compliant with all PCI DSS requirements.

Self-Assessment Questionnaire (SAQ): A validation tool for eligible organizations that self-assess their PCI DSS compliance and that are not required to submit a Report on Compliance (ROC). SAQs consist of two components: (1) a set of questions corresponding to the PCI DSS requirements designed for Merchants and service providers; and (2) an Attestation of Compliance or certification that the Merchant or Service Provider is eligible to perform and has performed the appropriate self-assessment. Different SAQs are available for various cardholder data processing environments; more details can be found at www.pcisecuritystandards.org.

Service Provider: A Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.

Third Party Vendor: A vendor with whom an Agency contracts (or intends to contract) for provision of services, including Cash Management services, selected by the Agency, and who is unaffiliated with Treasury for purposes of providing such services.

Validation of Compliance: The act of assessing and verifying the correct implementation of security controls, procedures, and policies as per the requirements of the PCI DSS. The validation process is two-fold: (1) pass applicable vulnerability scans at least quarterly; and (2) fully complete, annually, a Self-Assessment Questionnaire (SAQ).

Policy Statements

Agencies and Third Party Vendors that accept, transmit, process, or store customer Payment Card data or could impact security of cardholder data are contractually required to maintain compliance with all applicable requirements of the PCI DSS as participants in Treasury's Master Agreement for Merchant Card Services.

Notwithstanding any conflict with the Master Agreement, the following requirements are to be adhered to:

1. Agencies are required to validate PCI DSS compliance on an annual basis, with initial validation to occur no later than 90 days after merchant account approval.
2. Agencies are required to use a validation service that provides for the annual completion of the appropriate PCI DSS Security Assessment Questionnaire (SAQ), as required by the PCI DSS. Agencies have the following options to satisfy this requirement:
    a. Enroll in the validation service provided under Treasury's Master Agreement for Merchant Card Services; or

b. Procure a validation service offered by a Qualified Security Assessor (QSA).

3. Agencies that use one or more Payment Card acceptance methods involving external-facing IP addresses and domains, and are subject to undergoing quarterly vulnerability scans as required by the PCI DSS, are required to have external scans performed by an Approved Scanning Vendor (ASV). Agencies have the following options to satisfy this requirement:
   a. Enroll in the validation service, which includes vulnerability scanning, provided under Treasury's Master Agreement for Merchant Card Services, or
   b. Procure a vulnerability scanning service offered by an ASV.
4. Agencies are responsible for any cost related to their compliance with the PCI DSS, including but not limited to the annual completion of SAQs and vulnerability and penetration tests (if applicable). Agencies are further responsible for any costs associated with on-site security audits or forensic investigations that may be required.
5. Agencies that do not maintain an applicable validation service may not be allowed to access services through Treasury's Master Agreement for Merchant Card Services (per ORS 293.875, Treasury has *exclusive* authority to procure merchant card services on behalf of Agencies).
6. Agencies shall perform all requirements of the enrolled validation service in a timely manner in order to reflect and attest the status of compliance with the PCI DSS. Failure to comply with all requirements may result in Agencies being assessed fines or fees by the service.
7. Agencies shall provide reports reflecting and attesting the status of their compliance with the PCI DSS when requested by Treasury, the Acquirer, or central oversight agencies (*e.g.*, the OSCIO and Secretary of State).
   a. The Acquirer may use the information provided to determine an Agency's compliance status and to determine any rectifying action that the Acquirer deems appropriate to address any noncompliance issue. The Acquirer may address any noncompliance issue directly with Agencies and may assess Agencies fines or fees for noncompliance.
   b. Central oversight agencies may use the information for audit and compliance purposes or in response to a data breach or other data security incident.
8. Agencies notified by the Acquirer of a PCI DSS noncompliance issue must provide a response within the time frames provided by the Acquirer. Corrective actions must be taken that satisfies the Acquirer's concerns. Actions may include, but are not limited to, the following:
   a. Correcting the noncompliance issue within the time frame agreed to by the Acquirer;
   b. Implementing compensating measures agreed to by the Acquirer;
   c. Temporarily suspending the use of Payment Card acceptance until the noncompliance issue is resolved;
   d. Paying noncompliance fines or fees charged by the Acquirer;
   e. Discontinuing Payment Card acceptance as a payment method.
9. Agencies notified by the Acquirer of a PCI DSS noncompliance issue should seek guidance from a central oversight agency (*e.g.*, OSCIO) if subject to the central oversight agency's supervision.
10. Agency management is responsible for ensuring that the requirements of this policy are adhered to including, but not limited to, responding to any noncompliance issues that may arise.

Exceptions

None.

Failure to Comply

Failure to comply with these requirements may unnecessarily expose an Agency or Agency customers to losses due to financial fraud or negligence and may result in termination of an Agency's ability to conduct such transactions (per ORS 293.875, Treasury has *exclusive* authority to procure merchant card services on behalf of Agencies).

RESOURCES

- The PCI DSS may be viewed at the PCI Security Standards Council's website. *See* www.pcisecuritystandards.org
- Agencies interested in procuring a validation service in lieu of enrolling in the service provided under Treasury's Master Agreement for Merchant Card Services find the following resources useful:
  - The OSCIO's Basecamp Program provides public agencies an IT catalog that allows them to identify and contract for IT goods and services including PCI DSS services. *See* www.oregon.gov/basecamp/Pages/default.aspx
  - The PCI Security Standards Council manages programs that help facilitate the assessment of compliance with the PCI DSS: Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV). *See* www.pcisecuritystandards.org/assessors_and_solutions/

ADMINISTRATION

Feedback

Your comments are extremely important to improving the effectiveness of this policy. If you would like to comment on the provisions of this policy, you may do so by e-mailing Treasury at CustomerSolutions@ost.state.or.us. To ensure your comments are received without delay, *please list the policy number and name in your e-mail's subject*. Your comments will be reviewed during the policy revisions process and may result in changes to the policy.

Attachments:

Approval Signatures

Step Description	Approver	Date
	Cora Parker: Director of Finance	12/2019
	Carmen Leiva: Operations Analyst	12/2019
	Bryan González: Policy & Strategy Manager	12/2019