STOCKTON UNIVERSITY

Payment Card Industry Data Security Standard Compliance Program

Stockton University is committed to exercising best practices to protect customer cardholder data and to protect the University from cardholder breach by complying with the Payment Card Industry (PCI) Data Security Standard (DSS).

Purpose

The purpose of this document is to provide clear and manageable steps to ensure University-wide compliance with PCI standards.

Applicability and Responsibilities

This compliance program applies to all individuals who have responsibility, authority, and required by the PCI DSS. A log template can be found on the Fiscal Affairs website. A merchant should be able to immediately produce these logs upon request.

All secure online Payment Gateway technology (third-party vendor) must have a valid and up to date PCI DSS Attestation of Compliance (AOC). The AOC must be issued within the last year and reviewed on an annual basis. It is the responsibility of the department or organization using the Payment Gateway technology to obtain the AOC and submit it to the Controller.

Non-mobile credit card processing devices and systems must be

Disposition of Point-of-Sale Devices

University and Related Entities with Point-of-Sale devices or terminals that have been inactive for over two years shall dispose of the devices appropriately per PCI guidelines.

Helpful Resources

- PCI Security Standards Council https://www.pcisecuritystandards.org/
- PCI Security Standards Council Document Library https://www.pcisecuritystandards.org/document_library/?category=saqs&hsCtaTracking=126815f3-0b2c-4293-a0af-6537b9853828%7Cd83f0244-4bf7-49e8-822d-de40db9c272e
- Stockton University Information Security Plan https://stockton.edu/information-technology/documents/Information-Security-Plan.pdf
- Credit Card Acceptance by Departments https://stockton.edu/policy-procedure/documents/procedures/6419.pdf
- Identity Theft Prevention Program https://stockton.edu/policy-procedure/documents/procedures/6902.pdf

Appendix A: PCI DSS Definitions

Approved Scanning Vendor refers to a company qualified by the PCI Security Standard Council to conduct external vulnerability scanning services in accordance with PCI DSS.

Attestation of Compliance (AOC) is a report to attest to the results of a PCI DSS assessment and can be requested from a third-party vendor.

Cardholder Data is any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder Data includes the primary account number (PAN), which consists of a customer's 16-digit payment card number along with any of the following data types: cardholder name, expiration date, and card verification value.

Merchant means any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa)

Payment Application is approved software sold, distributed, or licensed which stores, processes, or transmits Cardholder Data as part of authorization or settlement. This includes customized, pre-installed, and "off-the-shelf" software.

payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation.

Personal Identification Number (PIN) is the personal number used in debit card transactions.

Point-of-Sale (POS) Hardware and/or software used to process payment card transactions at merchant locations.

Related Entities means the following types of entities and their subsidiaries: foundations, alumni associations, auxiliary enterprise corporations, college associations, student services corporations, performing arts centers, and art galleries, that accept payment cards using technology owned, operated, or made available by the University, such as servers, networks, hardware and software, and/or are using the name or trademark of the University or a constituent of the University, in connection with its operations.

Self-Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers report the results of their PCI DSS self-assessment. Different SAQs are specified for various methods of processing payment cards.

Third-Party Vendor (also called "third-party service provider") are business entities directly involved in transmitting, processing, or storing of Cardholder Data or which provides services that control or could impact the security of Cardholder Data.

Virtual Payment Terminals are web-browser-based access to a third-party service provider website to authorize payment card transactions when the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment.

Appendix B - Self-Assessment Questionnaires (SAQs)

There are different questionnaires available to meet different merchant environments.

SAQ	Description