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 stewardship over credit card or debit card payments processed by the University, and those who process credit or debit card payments on behalf of the University. The Controller is responsible for maintaining and overseeing compliance with this compliance program. Departments and campus organizations accepting payment cards should designate an individual responsible for compliance functions and for reporting back to the Controller. The Office of Information Security is responsible for reviewing the PCI DSS technical and network control requirements and, as necessary, will recommend the best practices to establish compliance. The Controller, in consultation with the Information Security Officer, is responsible for managing and, as necessary, revising the PCI DSS Compliance Program.

Merchant Registration Process

Departments looking to process credit card transactions on behalf of the University for the first time, in addition to Departments already processing credit card transactions that are interested in changing the existing processing environment must complete and submit to the Controller a Credit Card Processing Merchant Request Form. This form can be found on the Fiscal Affairs website. If approved, requestors are responsible for costs associated with credit card processing, software, and equipment.

Credit Card Readers and Online Payment Gateways

All payment processing systems and services must be reviewed and approved by the Office of Fiscal Affairs and Information Technology Services prior to use at the University. All credit card readers must be configured with Point-to-Point Encryption (P2PE) Solutions, as listed on the PCI Security Standards Council website.

University departments and Related Entities utilizing a Point-of-Sale (POS) device shall maintain an up-to-date device inventory log, which includes the device name, model, serial #, and location of the device(s), and shall periodically inspect the device for signs of skimming and tampering, as

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 connected directly (hard wired) to the University network. The security features intrinsic to the network will ensure compliance with the PCI DSS requirements related to a firewall, the use and regular update of anti-virus software or programs, assigning a unique ID for computer access, and system vulnerability scans.

Mobile or wireless credit card processing devices must communicate by way of a cellular connection and cannot connect over Wi-Fi. Users operating the devices are responsible for inspecting the device before each use to ensure the device is updated per vendor's instructions and functioning properly without compromise. The device should be physically secured when not in use to prevent unauthorized access.

Access to System Components containing Cardholder Data
University departments and Related Entities utilizing a system component handling Cardholder Data (i.e., Virtual Terminal or payment processing platform) shall assign a unique ID or username to each person with access and add and remove a person's access as needed. Access for users who separate from the University or whose job responsibilities no longer require such access shall be immediately revoked and removed.

As per PCI DSS requirements, passwords must, at least, have a minimum password length of seven characters and contain both numeric and alphabetic characters. University departments and Related Entities shall not use generic or shared user IDs and passwords and shall remove all generic user IDs prior to the utilization of the system component.

Processing Cardholder Data
It is preferred that cardholder data only be received in-person and processed through a credit card reader or online through a secure payment gateway.

If a payment card is accepted over the phone, do not write down card numbers on paper. The cardholder data must be entered directly into the payment processing software.

If payment card data is received by way of postal mail, it should be destroyed immediately after authorization. If not processed immediately, mail with cardholder data must be stored in a locked filing cabinet or safe, labeled "confidential" until processed. If a form containing cardholder data must be retained after transaction authorization based on a documented and justified business need, the cardholder data must be redacted using redacting pens. The form must be stored in a locked

filing cabinet or safe, labeled “confidential.” These forms shall not be retained for more than one year and shall be shredded, using a crosscut shredder.

University and Related Entities shall not accept Cardholder Data via end-user messaging technologies (i.e., email, text message, etc.), which are not secure means of transmission. Cardholder Data received via end-user messaging shall not be processed.

Cardholder data is classified as confidential information under the Stockton University Information Security Plan. A third-party vendor may store cardholder data for recurring donations/payments, as requested by the donor/patron. The third-party vendor secures this data.

Self-Assessment Questionnaire (SAQ) – *Merchant Requirement*
University departments and Related Entities that process payment cards must complete a SAQ annually to demonstrate compliance with PCI DSS. There are different questionnaires available to meet different merchant environments. Reference Appendix B. After review, please schedule a consultation with the Controller and Information Security Officer to ensure the appropriate SAQ is completed.

Internal and External Vulnerability Scans
Information Technology Services conducts regular internal and external vulnerability scans as a cybersecurity measure. Networks scans may be completed by a PCI-validated Approved Scanning Vendor when needed.

Annual PCI Awareness Training
All University and Related Entities staff with access to Cardholder Data are required to take the PCI Awareness training course upon hire and annually, thereafter. The Office of Human Resources will track completion.

Fraud Reporting
In the event of suspected fraud or data breach, notify the following University officials.

- Scott Huston, Chief Information Officer (Scott.Huston@stockton.edu)
- Demetrios Roubos, Information Security Officer (Demetrios.Roubos@stockton.edu)
- Brian Kowalski, General Counsel (Brian.Kowalski@stockton.edu)
- Jennifer Potter, Chief Financial Officer (Jennifer.Potter@stockton.edu)
- Stacey O’Brien, Controller (Stacey.O’Brien@stockton.edu)

Enforcement of Practices
Compliance with this program is required. Merchants that are out of compliance must address and resolve any deficiencies immediately. Merchants unable to maintain PCI Compliance will have their ability to accept credit cards suspended or revoked.

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%7Cd83f028f-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 card(s) mean credit and debit cards bearing the logo of major card brands, including Visa, MasterCard, American Express, Discover and JCB used to make a payment.

Payment Card Industry Data Security Standard (PCI DSS) refers to a set of technical and operational requirements established by the PCI-SSC designed to protect account data and applies to all entities involved in payment card processing – including merchants, processors, acquirers, and service providers.

Payment Card Industry Security Standards Council *was* founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc., whose mission is to enhance global

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 a 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
A	Card-not-present merchants (e-commerce or mail/telephone-order) that completely outsource all account data functions to PCI DSS validated and compliant third parties. No electronic storage, processing, or transmission of account data on their systems or premises. *Not applicable to face-to-face channels. Not applicable to service providers.*
A-EP	E-commerce merchants that partially outsource payment processing to PCI DSS validated and compliant third parties, and with a website(s) that does not itself receive account data, but which does affect the security of the payment transaction and/or the integrity of the page that accepts the customer's account data. No electronic storage, processing, or transmission of account data on the merchant's systems or premises. *Applicable only to e-commerce channels. Not applicable to service providers.*

SAQ	Description
B	Merchants using only: • Imprint machines with no electronic account data storage, and/or • Standalone, dial-out terminals with no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
B-IP	Merchants using only standalone, PCI-listed approved PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor. No electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
C-VT	Merchants that manually enter payment account data a single transaction at a time via a keyboard into a PCI DSS validated and compliant third-party virtual payment terminal solution, with an isolated computing device and a securely connected web browser. No electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
C	Merchants with payment application systems connected to the Internet, no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
P2PE	Merchants using only a validated, PCI-listed Point-to-Point Encryption (P2PE) solution. No access to clear-text account data and no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
SPoC*	Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions. No access to clear-text account data and no electronic account data storage. *Not applicable to unattended card-present, mail-order/telephone order (MOTO), or e-commerce channels.* *Not applicable to service providers.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types. *Not applicable to service providers.*
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete an SAQ.