ACCOUNTING PROCEDURES – GENERAL
Section: 300 - 86
Effective: 10/17/2017
Supersedes: N/A New
Review Date: 10/17/2020
Issuance Date: 10/17/2017
Issuing Office: Business & Financial Services, General Accounting Division

Payment Card Processing and Compliance Policy

I. SCOPE

This policy applies to any person or entity that, on behalf of UC San Diego, handles, processes, transmits, or stores cardholder data in a physical or electronic format.

II. POLICY SUMMARY

The Payment Card Industry Security Standards Council (PCI SSC) maintains strict security requirements to safeguard credit or debit payment cardholder data through mandated Payment Card Industry Data Security Standards (PCI DSS).

Compliance with PCI DSS is required by the PCI SSC and by University of California Business and Finance Bulletin No. BUS-49, "Policy for Cash and Cash Equivalents Received."

III. DEFINITIONS

Attestation of Scan Compliance (AOSC) - The Attestation of Scan Compliance is an overall summary that shows whether the scan customer's infrastructure received a passing scan and met the scan validation requirement. An AOSC is part of the annual Payment Card Industry (PCI) report and is also done periodically throughout the year.

Cardholder data is any personally identifiable data associated with a payment cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, and Card Validation Code – a three-digit or four-digit value printed on the front or back of a payment card referred to as CAV, CVC, CVV, or CSC depending on the payment card brand.

Merchant refers to any UC San Diego department or operating unit that has applied for and been approved to accept credit/debit card payments for goods and/or services.

Payment Card refers to both credit and debit cards. This policy does not apply to the UC San Diego P-card or corporate card programs.

Payment Card Processing - The use of any application or device to process a credit/debit card transaction as payment for goods or services purchased from a Merchant.

PCI DSS - Payment Card Industry Data Security Standard.

PCI Security Standards Council (PCI SSC) - The Security Standards Council defines credentials and qualifications for assessors and vendors and maintains the PCI-DSS.

Qualified Security Assessor (QSA) - A company that is an independent security organization certified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS.

QSA Employees are individuals employed by a QSA that have satisfied and continue to satisfy all QSA Requirements.

PCI Self-Assessment Questionnaire (SAQ) - a questionnaire promulgated by the PCI, which Merchants use to demonstrate compliance to the PCI DSS and to the payment processor.

UC San Diego - UC San Diego campus, UC San Diego locations, and UC San Diego Health.

IV. POLICY STATEMENT

It is in the best interests of, and operationally vital for, UC San Diego and our customers to continuously comply with PCI DSS.

This policy is structured to:

1. Define requirements and responsibilities to establish and maintain a UC San Diego merchant account to process payment cards and remain in compliance with PCI DSS.

UC San Diego has a responsibility to our customers and payment card processors to comply with the PCI DSS when processing payment card transactions. Non-compliance with PCI-DSS can result in serious consequences for UC San Diego, including reputational damage, loss of customers, litigation, and financial costs.

The purpose of this policy is to:

1. Ensure ongoing compliance with PCI DSS and other applicable policies and standards,
2. Establish the governance structure for payment card processing and compliance activities at UC San Diego,
3. Define responsibilities for payment card services to various UC San Diego constituents, and
4. Provide general guidelines regarding the handling of cardholder data.

All technical and operational system components involved in processing cardholder data are subject to PCI DSS and to this policy. These include owned or leased software, hardware, computers and wired or wireless electronic devices.

V. RESPONSIBILITIES

The Vice Chancellor – Chief Financial Officer (CFO) has overall PCI DSS compliance authority for UC San Diego. The CFO hereby delegates authority to the Controller the authority to define responsibilities for payment card services to UC San Diego constituents.

UC San Diego's PCI DSS compliance is a consolidated attestation of compliance. Consequently, one Merchant who fails to meet PCI DSS requirements causes the entire institution to be out of compliance. Therefore, failure of any single Merchant to maintain continuous PCI-DSS compliance will result in immediate cancellation of that merchant account to preserve and allow continuous operations for other critical business functions dependent on payment cards.

1. Office of Internal Controls & Accounting (General Accounting):

a. The UC San Diego Payment Card Coordinator within General Accounting is responsible for initiating and overseeing the annual PCI DSS validation, making appropriate revisions to this policy as needed, and coordinating any remediation activities as required by PCI DSS or other applicable policies and standards.

b. The UC San Diego Payment Card Coordinator is responsible for supporting and approving initial setup and ongoing administration of PCI DSS compliance for all UC San Diego merchant accounts. Key responsibilities include approval of merchant applications, facilitating procurement of credit card terminals and other equipment, and operational liaison to UC San Diego's third-party credit card processing vendor, QSA, and forensics vendor.

c. The UC San Diego Payment Card Coordinator will certify overall UC San Diego PCI DSS compliance to the QSA on behalf of UC San Diego after individual Merchants successfully complete their PCI DSS attestations on or before the annual PCI DSS certification due date as established by Bank of America Merchant Services.

d. The UC San Diego Payment Card Coordinator will notify each Merchant with reasonable notice to complete and submit the annual departmental PCI DSS assessment. Accurate and timely completion of this assessment is the responsibility of the PCI Department Coordinator. The PCI Department Coordinator must complete the SAQ annually, after remediation of a breach of data, or anytime a credit card related system or process changes.

2. **Information Technology Services (ITS):**

a. Responsible for maintaining and disseminating security policies and procedures that address PCI DSS requirements, establishing and testing UC San Diego's infrastructure and network environment, and assisting the Payment Card Coordinator and UC San Diego merchants in completing the technical sections of the annual SAQ. ITS will work closely with the UC San Diego QSA to interpret PCI DSS requirements and to communicate and facilitate overall security and technical compliance with Merchants.

b. Responsible for configuration and maintenance of centralized IT systems, facilitating merchant hardware and software configurations, and providing oversight of all computer systems and other IT resources to support compliance with PCI DSS and UC security requirements. ITS will manage and provide training and tools to limit access to IT resources and cardholder data, and assist the Office of Internal Controls & Accounting and individual Merchants in completing the technical sections of the annual SAQ.

c. ITS, shall provide information technology sufficient to fully support enforcement of this policy. Additionally, ITS will support investigation conducted by a third-party forensics vendor and remediation of any reported violations of this policy, and will lead investigations about credit card security breaches with support from UC San Diego's on-call forensics contractor and may terminate access to protected information of any users who fail to comply with the policy.

3. Business & Financial Services Procurement & Contracts Division:

Is responsible for ensuring inclusion of appropriate PCI DSS requirements clauses in all vendor and external entity contracts to ensure assignment of accountability for these policy requirements where PCI DSS applies for the goods or services being acquired by UC San Diego or its agents. See the University's Data Security and Privacy Appendix as part of the UC Systemwide Templates & Documents

4. **Merchants:**

a. Are responsible for ensuring that all business processes, IT environments and associated systems for accepting, processing, retaining, and disposing of cardholder data comply with PCI DSS.

b. Are responsible for performing an annual SAQ in partnership with Internal Controls & Accounting and ITS. Departmental employees who handle cardholder data must attend a UC San Diego annual security awareness & training program and sign the Payment

Card Merchant Compliance Statement (Appendix A). Merchant account holders who fail to comply are subject to:

i. Any fines imposed by the payment card industry;

ii. Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees; and

iii. Suspension of the merchant account.

c. Who are required by PCI DSS to conduct periodic vulnerability scans shall download, review and retain the Attestation of Scan Compliance (AOSC) as evidence of scan pass and immediately apply resolution processes to bring the Merchant environment back into compliance if the AOSC fails.

d. Are required to conduct penetration testing as defined by PCI DSS. The Merchant will complete relevant components of the rules of engagement and/or penetration test charter requirements by the due dates provided by the QSA. Additionally, affected Merchants will perform due diligence checks on the inclusion/exclusion lists, ensuring these lists are accurate and properly vetted. Any vulnerabilities identified by the penetration tests will be reviewed for further action. Absence of compensating controls or those deemed inadequate, will require the Merchant to patch the vulnerability in a timely fashion. Evidence of remediation will be made available to the penetration testers and is subject to independent verification.

e. Are required to adopt PCI DSS validated Point-to-Point Encryption Technologies (P2PE). UC San Diego's preferred P2PE solution is provided by Bluefin Payment Systems. And with the Office of Internal Controls and Accounting (General Accounting) approval through consultation with the Chief Information Officer(s) for UC San Diego, other PCI DSS validated P2PE solutions may be adopted to support unique merchant payment processing requirements. Alternatives to the preferred solution may bring more risk to UC San Diego, and therefore will be highly scrutinized.

f. Are required to protect cardholder data on paper. Physical, unsecured storage of cardholder data on paper is prohibited. Once the credit card payment is processed, all paper cardholder data shall immediately be destroyed. Cardholder data will not be transmitted or received by email, fax or text messaging.

VI. PROCEDURES

UC San Diego's procedures for establishing a merchant account and maintaining PCI compliance equipped to accept and process payment cards at UC San Diego are maintained on our Blink pages here. Procedures detailed on Blink provide a wide range of information, guidelines, and resources related to credit and debit card processing at UC San Diego. Blink provides Merchants with the information and resources needed to support this policy and process credit and debit card payments in compliance with current PCI DSS.

VII. FORMS

Appendix A: Payment Card Merchant Compliance Statement

VIII. RELATED INFORMATION

A. University of California Business and Finance Bulletin - Policy for Cash and Cash Equivalents Received (BUS-49)

B. University of California Business and Finance Bulletin IS-3 Electronic Information Security

C. UC San Diego PPM 135-3 Network Security Policy

D. UC San Diego Implementation Plan for Protection of Electronic Personal Identity Information

E. Blink - Credit & Debit Card Processing at UC San Diego

F. The PCI Security Standards Council

IX. REVISION HISTORY

None new policy

ACCOUNTING PROCEDURES – GENERAL
Section: 300 - 86 APPENDIX A
Effective: 10/17/2017
Supersedes: N/A New
Review Date: 10/17/2020
Issuance Date: 10/17/2017
Issuing Office: Business & Financial Services, General Accounting Division

Payment Card Merchant Compliance Statement

As a UC San Diego employee with responsibilities for handling payment cards and cardholder data, I recognize that I have access to sensitive and confidential information. I will strive to protect UC San Diego and its customers at all times when making decisions concerning payment cards and cardholder data, and I agree with the following statements:

- I have read, understand, and agree to abide by UC San Diego's Payment Card Processing and Compliance Policy, related guidelines in Blink, and other related policies, including: Network Security Policies, Electronic Personal Identity Information, BUS-49 Policy for Cash and Cash Equivalents Received, IS-3 Electronic Information Security.
- I will continually strive to ensure our merchant cardholder data environment (CDE) is in continuous compliance with laws, rules, and policies governing the processing of card payments, including PCI DSS requirements.
- I will provide the Payment Card Coordinator with all requested documentation for verification of ongoing PCI DSS compliance.
- I will inform the Payment Card Coordinator promptly of any changes to the Cardholder Data Environment (CDE).
- I will maintain an accurate equipment inventory log for equipment associated with the CDE.
- I will utilize cardholder data for UC San Diego business purposes only.
- I will not use or distribute cardholder data for personal purposes. I understand that such actions are illegal and grounds for prosecution.
- I understand that in cases where I suspect a breach of security, including the suspicion that cardholder data has been exposed, lost, stolen, or misused, I must immediately contact UC San Diego General Accounting and ITS Information Security.
- I understand that I must maintain effective business processes for accepting, processing, retaining, and disposing of cardholder data.
- I understand that failure to comply with this policy and applicable policies, standards, and procedures may include loss of the ability to process payment card transactions and disciplinary action, which can include termination of employment.

Employee Name:		
Print Name	Signature	Date
Employee ID Number:	Department Name:	
Department Manager Approver:		
Print Name	Signature	Date