1.0 Introduction

This standard provides guidance to ensure that credit card acceptance and ecommerce processes comply with the Payment Card Industry Data Security Standards (PCI DSS) and are appropriately integrated with the University's financial and other systems. Such actions protect the interests of the University, its associated Auxiliaries, and its customers. This standard applies to all types of credit card activity transacted in-person, over the phone, via fax, mail or on the Internet.

2.0 Payment Card Industry Data Security Standard (PCI-DSS)

The campus and all departments that process credit or debit card information must comply with the Payment Card Industry Data Security Standards (PCI DSS). This includes the acquiring, accepting, capturing, storing, processing or transmitting of credit or debit card data, in both electronic and non-electronic formats.

PCI DSS is a set of comprehensive requirements for enhancing credit card data security. PCI data security standards were developed by the PCI Security Standards Council, and a single violation of any of the requirements can trigger an overall non-compliant status. Each non-compliant incident may result in steep fines, suspension and revocation of card processing privileges.

Although the primary focus of the PCI DSS is on web-based sales and processing credit card information via the Internet, there are other processes that allow systems to be Internet accessible, which may expose cardholder information. All campus credit card merchants, including merchants transmitting via a terminal on a dedicated phone line, or other approved method of transmission must complete an annual self-assessment survey and, if applicable, an internal scan and a remote external scan by a PCI DSS approved vendor.

3.0 Scope

Any college, department, auxiliary organization, entity or individual that in any way accepts, captures, stores, processes or transmits credit or debit card information, using campus information assets, (both electronic and non-electronic), or uses third-party service providers to do this for you; is governed by this Information Security Standard.

4.0 Credit Card Policies and Credit Card Acceptance Procedure

ICSUAM 6340 requires that the campus CFO or designee approve all physical locations, websites, third-party processor, or any channel accepting credit card payments. Any change involving credit card acceptance must first be approved by the CFO or his/her designee.

The Sacramento State Credit Card Acceptance Procedure must be followed prior to any addition or modification to credit card acceptance.

5.0 Roles & Responsibilities

The University Chief Financial Officer or his/her designee, and the Bursar are responsible for the administration of Credit Card Procedures. *See Sacramento State Credit Card Acceptance Procedures.*

The Information Security Officer is responsible for coordinating the University's compliance with the PCI Data Security Standards technical requirements.

6.0 Department Responsibilities

It is the responsibility of the Appropriate Administrator to ensure compliance with the campus standards for accepting credit cards. Departments will meet the following administrative requirements:

6.1 Ensure that all employees, contractors, and agents with access to payment card data within the relative department complete appropriate training, and acknowledge on an annual basis, in writing, that they have read and understood relevant policies and standards.

6.2 Perform background checks – Departments must perform applicable background checks on potential employees who have access to systems, networks, or cardholder data within the limits of Sacramento State HR policy, union bargaining agreements and local law. If employees have access to one card number at a time to facilitate a transaction, such as store cashiers, background checks are not necessary.

6.4 Document departmental credit card payment flows for each method, channel or business process where credit cards are accepted. Sample credit card payment flows are located on the Sacramento State PCI-DSS Website.

6.5 Complete the appropriate Sacramento State Annual Credit Card Security Self-Assessment Questionnaire and forward it to the Information Security Office (ISO) at

iso@csus.edu, for review. Questionnaires are located on the Sacramento State PCI-DSS Website.

6.6 Provide up-to-date annual assessment documents and PCI certifications to ISO.

6.7 Maintain department credit card security handling procedure that comply with the PCI DSS. In addition to complying with campus information security policy and standards, departments should establish procedures for physically and electronically safeguarding cardholder information. Exceptions to these policies and procedures may be granted with written approval from an appropriate administrator.

6.8 Communicate procedures to staff – Appropriate administrators should communicate the department credit card security handling procedures to staff and ensure that the "Credit Card Handlers and Processors Responsibilities" section of this standard is followed for all personnel involved in credit card transactions.

7.0 Business Unit Requirements

7.1 **Prevent unauthorized access to cardholder data and secure the data**: Appropriate administrators should establish procedures to prevent access to cardholder data in physical or electronic form. Hard copy or media containing credit card information should be stored in a locked drawer or office, and password protection should be used on computers.

7.2 **Restrict access based on a business need-to-know**: Access to physical or electronic cardholder data should be restricted to individuals whose job requires access. Appropriate administrators should establish appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.

7.3 **Assign a unique ID to each person with computer access**: Departments should ensure that a unique ID is assigned to each person with computer access to credit card information. User names and passwords may not be shared.

7.4 **Transmitting credit card information by e-mail or fax**: Full or partial credit card numbers and three-or-four-digit validation codes (usually on the back of credit cards) may **not** be faxed without specific approval. Card holder data or full credit card number must not be stored electronically including via email. Partial credit card numbers may be stored or transferred in electronic format.

7.5 **Never store electronically the CVV, CVV2 validation code, or PIN number**: Departments must not store the three or four-digit CVV or CVV2 validation code from the credit card or the personal identification number (PIN).

7.6 **Mask 12 of the 16 digits of the credit card number**: Terminals and computers must mask all but the first 6 digits and/or the last 4 digits of the credit card number (masking all digits but the last 4 is standard practice on campus).

7.7 **Using imprint machines**: Imprint machines need special handling as they display the full 16-digit credit card number on the customer copy. Departments should not use imprint machines to process credit card payments unless personnel have been authorized to do so, and processes exist to securely store and dispose of the information.

7.8 **Departments must maintain a list of all devices used to processes credit cards.**

7.9 **Departments must maintain a list of all vendors and vendor applications** used to process credit cards.

7.10 **Use of personal computers to process credit cards using "card swipes" or keyboard entry is prohibited** without prior approval and must be network isolated (with ingress and egress rules) and must be a single-use system.

7.11 **In the event of a suspected or confirmed loss of cardholder data**, immediately notify the Information Security Office (iso@csus.edu) and the Bursar's Office. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notify University Police at (916) 278-6851.

8.0 Technical Requirements

*Staff or faculty with access to credit or debit card holder data **must not**:*

8.1 Acquire or disclose any cardholder's credit card information without the cardholder's consent including but not limited to the full or partial sixteen (16) digit credit card number, three (3) or four (4) digit validation code (usually on the back of credit cards), or PINs (personal identification numbers).

8.2 Transmit or request any credit card information by e-mail or fax. If someone e-mails their data, staff and faculty should make them aware that, for their own safety, they should not do this again. The email or fax should be destroyed as soon as possible.

8.3 Electronically store or record any credit card information in any electronic format (Excel files, databases, e-mail, etc.) unless they have been authorized to do so by the Information Security Office.

8.4 Request, record, or store any of the magnetic stripe data or the credit card confirmation code (three-digit on the back of many cards and 4 digits on the front of American Express).

8.5 Share a computer password if they have access to a computer with credit card information.

*Staff or faculty with access to credit or debit card holder data **should**:*

8.6 Change a vendor-supplied or default password if they have access to a computer with credit card information.

8.7 Password protect their computer if they have access to a computer with credit card information.

8.8 Store all non-electronic, physical documents or storage media containing credit card information in a locked drawer, locked file cabinet, or locked office.

8.9 Store all electronic files on a secured server, or as encrypted or password protected files.

8.10 Review devices which are used to process credit cards for tampering.

8.11 Report immediately a credit card security incident to an appropriate administrator if it's known or suspected credit card information has been exposed, stolen, or misused and immediately notify the Information Security Office at iso@csus.edu.

8.12 Store only essential credit card information. Any stored information must be destroyed in accordance with the campus Record Retention Schedule. All media used for credit cards must be destroyed when retired from use. All hardcopies must be shredded prior to disposal.

9.0 Storage & Processing of Credit Card Data

9.1 Storage of credit card numbers on University-owned computers, servers, or in University developed applications is prohibited.

9.2 Storage of credit cardholder data in non-electronic (faxes, imprint machine slips, handwritten forms, etc.) data must follow cash handling standards.

9.3 Non-credit card terminal devices of any kind that process or "card swipe" or enter data using a keyboard must use tokenization or Point-to-Point Encryption (P2PE) technologies that meet PCI-P2PE requirements.

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)	Version
5/04/2019	Information Security Office	Reviewed and Recommended	V1.0
7/19/2019	PCI Committee	Approved	V1.1
2/22/2021	IRT, AITC	Receive comments/feedback from AITC.	V1.1
3/1/2021	IRT, Director of Policy and Records Management	Recommended for approval/publication.	V1.1