1.0 Introduction

This document establishes procedures related to credit card payments in accordance with ICSUAM Policy 6340.00 and the Payment Card Industry (PCI) Data Security Standards. Any department at Sacramento State wanting to accept credit cards for payment of goods or services must obtain approval prior to doing so and must agree to meet the requirements of the PCI Data Security Standard. These procedures govern the process by which University departments request approval from the Associate Vice President for Financial Services/University Bursar to accept credit card payments deposited with the University.

2.0 Administration

The University Chief Financial Officer and his/her designee, the University Bursar and Information Security Officer, are responsible for the administration of these procedures.

3.0 Scope

These procedures apply to any University or Auxiliary department accepting credit cards for goods or services provided. University and Auxiliary departments shall request authorization to accept credit cards via the procedures included in this document and to ensure compliance.

4.0 Background

California State University and its auxiliaries are required to comply with the Payment Card Industry Data Security Standard. The standard was developed by the major credit card companies as requirements a business must adhere to when accepting credit cards. A business risks losing the right to process credit card payments and being audited and/or fined for noncompliance. Therefore, University departments must obtain approval and appropriate training prior to accepting credit cards for payment. Failure to do so may result in the department being denied the right to accept credit card payments.

5.0 Authorization to Add or Modify Credit Card Acceptance Channel

ICSUAM 6340.00 requires that the campus CFO or designee approve all physical locations, websites, 3rd 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 following is the process to request authorization or modification for accepting credit card payments for the campus.

1. Read the guidelines and requirements of the Payment Card Industry (PCI) Data Security Standard (DSS) and the Sacramento State Credit Card Acceptance Security Standards as they apply to the university and your department accepting credit card payments.
2. Complete the Credit Card Channel Acceptance Form, obtain the approval and signature of the appropriate Dean or Program Center Administrator and submit to the University Bursar for authorization.
3. Within 10 working days of receipt of the request, the University Bursar will inform you in writing the acceptance or denial of your request.

6.0 Roles and Responsibilities

6.1 Business Unit Functional Contact

The person who manages the credit card acceptance process for the department or business unit. Generally a project director, unit supervisor or program coordinator.

6.2 Business Unit Responsible Administrator

An MPP or administrator who is responsible for the department or business unit. Generally a college dean or equivalent.

6.3 Department

It is the responsibility of the Business Unit Responsible Administrator to ensure compliance with the campus procedures for accepting credit cards. Failure to comply with the University procedures and requirements of the PCI Data Security Standard will risk a department’s approval to accept credit card payments, and may result in removal of authorization. Business Unit Responsible Administrators should identify Business Unit Functional Contacts, who should develop procedures, document card acceptance processes, and coordinate compliance efforts for the business unit.

Business Unit Responsible Administrators are responsible for the following:

- Ensure that all individuals 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 procedures.
- Ensure that all individuals with access to payment card data within the relative department maintain a clear background check status. Some employees may have direct supervisors outside of the business unit for whom they work. In this case, the Business Unit Responsible Administrator must work with the outside supervisor to ensure a clear background check status. Some employees may have been grandfathered in when background checks were not required. These employees may only have access to one card number at a time to facilitate a transaction.

- Document Stateside or Auxiliary Organization departmental credit card handling procedures for each method, channel or business process where credit cards are accepted.
- Participate in the annual PCI compliance assessment with the Information Security & Bursars Offices.
- Provide up to date annual assessment documents and PCI certifications to Information Security.
- Be responsible for credit card fees which will be charged to a Stateside PeopleSoft (CFS) or Auxiliary Organization general ledger account identified by the department.
- ADD CASH HANDLING & ACCOUNTING (ABA) SOD, Refunds – reconciliation SOD.
- Ensure that all payment card data collected by the relevant department in the course of performing University business, regardless of whether the data is stored physically or electronically, is secured according to the standard listed in the Sacramento State PCI Data Security Standard Compliance.
- In the event of a suspected or confirmed loss of cardholder data, immediately notify the Information Security Office and the Student Financial Services 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.

If the Business Unit Responsible Administrator is no longer able or available to ensure compliance with the procedures and requirements for accepting credit cards, a new Credit Card Acceptance Business Inventory Form must be submitted immediately. Failure to do so will risk a department's approval to accept credit card payments, and may result in the removal of authorization.

6.4 Bursars Office

The University Chief Financial Officer and his/her designee, and the AVP for Financial Services, are responsible for the business and accounting related compliance with ICSUAM 6340.00 and administration of these procedures. The Bursars Office will approve all physical locations, websites, third-party processors, or any channel accepting credit card payments. Additionally, the Bursars Office will:

- Approve requests from campus departments before credit cards can be accepted.
- Maintain process for stateside departments accepting credit cards.
- Provide appropriate cash handling training for stateside departments.

- Reconcile stateside merchant credit card activity to the Common Financial System at least monthly.
- Ensure that stateside credit card processing fees are properly charged back to the appropriate Department in accordance with relevant contracts.
- Process all stateside credit card refunds. When a good or service is purchased using a payment card and a refund is necessary, the refund must be credited back to the account that was originally charged.
- Generally, refunds back to the card will be processed for up to six months after the original transaction date. Refunds in excess of the original sale amount or cash refunds are prohibited.
- Process chargebacks for stateside departments and the department will provide appropriate supporting documentation.

6.5 Information Security Office

The University will be responsible for maintaining an Information Security Policy and guidelines as they apply to the acceptance of credit card payments; including an annual review of all University departments and entities accepting credit card payments to ensure compliance.

The Information Security Office will:

- Evaluate technical and security components of credit card acceptance requests.
- Maintain the PCI portal.
- Provide guidance and coordination during the PCI inventory.
- Report the compliance status for each division.
- Coordinate training enrollment activities with the business units.

7.0 Information & Restrictions

Prohibited Payment Card Activities

CSU prohibits certain credit card activities that include, but are not limited to:

- Accepting payment cards for cash advances.
- Discounting a good or service based on the method of payment.
- Adding a surcharge or additional fee to payment card transactions without approval from Bursar’s Office for Stateside transactions, or appropriate administrator for Auxiliary Organization transactions.

Training

Employees who are expected to be given access to cardholder data will initially be required to complete security awareness and PCI training. Employees will be required to acknowledge at least annually that they have received training, understand cardholder security requirements, and agree to comply with these procedures.

Background Checks
Departments are required to perform background checks on potential employees who have access to systems, networks, or cardholder data within the limits of CSU and CSU 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 recommended but are not required.

8.0 Cross References

Below are policies and standards that can be referenced as possible resources in implementing this process:

- Bank Accounts and Cash Management
- Conditions of Maintenance of Good Standing by Auxiliary Organizations at Sacramento State
- Delegated Financial Authority and Responsibilities
- Non-State Funds, Accepting and Administering

ICSUAM Policy 6340.00
Payment Card Industry (PCI) Data Security Standards (DSS)
Sacramento State Credit Card Handling Security Standard

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