California State University
SAN MARCOS

Finance &
Administrative
Services

**Business and Financial Services** California State University San Marcos 333 S. Twin Oaks Valley Road San Marcos, CA 92096-0001
**Tel:** 760.750.4473 www.csusm.edu/bfs/index.html

# Credit/Debit Card Acceptance Procedures

## Purpose

This document establishes CSU San Marcos procedures related to credit/debit card payments in accordance with ICSUAM Policy 6340.00 and the Payment Card Industry (PCI) Data Security Standards. Any department at CSU San Marcos wanting to accept credit/debit 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 campus CFO or their designee to accept credit/debit card payments deposited with the university.

## Administration

The university CFO and their designee are responsible for the administration of these procedures.

## Summary

These procedures apply to any university or auxiliary department accepting credit/debit cards at physical locations, websites, 3rd party processors, or any channel accepting credit/debit card payments. University and auxiliary departments shall request authorization to accept credit/debit cards via the procedures outlined in this document and are responsible for compliance. Credit/debit card payments can only be accepted at approved locations, using an approved CSU merchant card processor.

## Authorization to Add or Modify Credit/Debit Card Acceptance Channel

ICSUAM 6340.00 requires the campus CFO or designee approve all locations wishing to accept credit/debit card payments. Establishing credit/debit card acceptance, or any change to an existing location, must first be approved by the CFO or their designee. To request authorization or modification, a department/location must:

1. Review the roles and responsibilities within this document and determine obligations.

2. Complete the Credit/Debit Card Channel Request Form, obtain the approval and signature of the appropriate responsible manager, and submit to the Director of Student Financial Services for authorization.

3. The request will be evaluated and may require additional compliance documentation.

## Roles

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

Responsible Manager: MPP or administrator who is responsible for the department or business unit. Typically a college dean or equivalent.

## Responsibilities

**Responsible Managers** are responsible to ensure compliance with the campus procedures for accepting credit/debit 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/debit card payments and may result in removal of authorization.

Responsible Managers should identify Functional Contacts. Functional Contacts should develop procedures, document card acceptance processes that comply with the university's procedures.

In addition to compliance, Responsible Managers are responsible for the following:

- Ensure that all individuals with access to payment card data 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 have characteristics to accept responsibility/accountability.
- Document stateside or auxiliary organization departmental credit/debit card handling procedures for each method, channel, or business process where credit/debit cards are accepted.
- Participate in the annual PCI compliance assessment with IITS Information Security.
- Provide up to date annual assessment documents and PCI certifications to IITS Information Security.
- Be responsible for credit/debit card fees which will be charged to a stateside or auxiliary general ledger account identified by the department.
- 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 PCI standards listed in this document
- In the event of a suspected or confirmed loss of cardholder data, immediately notify IITS and Student Financial Services. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notification shall be made to University Police at 760-750-4567.

If the Responsible Manager is no longer able or available to ensure compliance with the procedures and requirements for accepting credit cards, a new Credit/Debit Card Channel Acceptance 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.

**IITS Information Security Department** is responsible for coordinating the university's compliance with PCI Data Security Standards technical requirements. Information Security will coordinate an annual review of all university departments and entities accepting credit/debit card payments to ensure compliance with credit/debit card handling security standards. Information Security will maintain copies of each department's self-assessments and annual certifications of compliance documentation. Information Security will coordinate PCI-DSS training for all locations.

**The University Chief Financial Officer, and their designee**, are responsible for the business and accounting related compliance with ICSUAM 6340.00 and administration of these procedures. The CFO or their designee will approve all physical locations, websites, 3rd party processors, or any channel accepting credit card payments.

**Student Financial Services will:**

- Provide notification to departments of approvals to accept credit/debit cards.
- Provide appropriate cash handling training for stateside departments.
- Process all stateside credit/debit card refunds. When a credit/debit card 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.

**Fiscal Services** will reconcile stateside merchant card activity to the Common Financial System at least monthly and ensure that stateside credit/debit card processing fees are properly charged back to the appropriate department in accordance with relevant contracts.

## Restrictions

California State University prohibits certain credit/debit card activities that include, but are not limited to:

- Accepting payment cards for cash advances
- Discounting a good or service based on method of payment
- Adding a surcharge or additional fee to payment card transactions without approval from the CFO or their designee for stateside transactions, or appropriate administrator for auxiliary organization transactions