CALIFORNIA STATE UNIVERSITY CHICO
FINANCIAL SERVICES

STUDENT FINANCIAL SERVICES
STUDENT SERVICES CENTER
ROOM 230
CHICO, CA 95929-0242
530-898-5936
www.csuchico.edu/sfin

Credit Card Acceptance Procedures

PURPOSE:
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 CSU Chico 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 Director of Student Financial Services to accept credit card payments deposited with the University.

ADMINISTRATION:
The University Chief Financial Officer and his/her designee, the Director of Student Financial Services, are responsible for the administration of these procedures.

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.

BACKGROUND:
California State University, Chico 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.

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. Complete the Credit Card Channel Acceptance Form, obtain the approval and signature of the appropriate Responsible Administrator, and submit to the Director of Student Financial Services for authorization.

2. Read the CSU Chico PCI Data Security Standard Compliance (ISEC) Requirements and determine the department obligations.

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

ROLES AND RESPONSIBILITIES:
Definitions
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.
2. Business Unit Responsible Administrator – an MPP or administrator who is responsible for the department or business unit. Generally a college dean or equivalent.

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. Business Unit Functional Contacts 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 which 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 ISEC.
- Provide up to date annual assessment documents and PCI certifications to ISEC.
- 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.
- 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 CSU, Chico 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, notification shall be made to University Police at (530) 898-5555.

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.

Information Security Department (ISEC)

ISEC is responsible for coordinating the university's compliance with the PCI Data Security Standards technical requirements. ISEC will coordinate an annual review of all University departments and entities accepting credit card payments to ensure compliance with the campus CSU Chico, Credit Card Handling Security Standards. ISEC will maintain copies of each department's annual assessment documents as well as Self Assessments and annual certifications of compliance. ISEC will coordinate PCI-DSS training for all locations.

Student Financial Services (SFIN)

The University Chief Financial Officer and his/her designee, the Director of Student Financial Services, are responsible for the business and accounting related compliance with ICSUAM 6340.00 and administration of these procedures. SFIN will approve all physical locations, websites, 3rd party processors, or any channel accepting credit card payments. Additionally, SFIN 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.

INFORMATION AND RESTRICTIONS:

Prohibited Payment Card Activities

California State University 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 SFIN for Stateside transactions, or appropriate administrator for Auxiliary Organization transactions

Training

Employees who are expected to be given access to cardholder data shall initially be required to complete security awareness and PCI training and then renew that awareness training at least annually. Employees shall 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 not required.

REFERENCES:

Cash Management Procedures
PCI-DSS Data Security Standards
ICSUAM Policy 6340.00 – Debit/Credit Card Payment Policy
Exception Justification - ISEC

Original Implementation Date: July 2015
Revision Date: July 2018