Application for New Payment Card Merchants

Last Revision Date: April 7, 2023

General Description

Purpose:

To be completed by departments that would like to accept payment cards (Visa, Master Card, American Express, Discover cards, and debit cards) as a form of payment for goods and/or services, receipt of donations, non-tuition courses, conferences, seminars, tickets and other approved California State University Bakersfield related products.

Please read Payment Card Handling Policy ({INSERT LINK}) and Payment Card Procedures ({INSERT LINK}) prior to completing this application to make sure that your department will be able to comply with all the requirements listed in this Policy.

Application must be submitted to CSUB PCI Committee. Once the application has been approved, please allow at least four weeks for electronic terminals and eight weeks for web-based setup prior to the desired "live" date. The information provided on this application will be used to create an "Information Profile" that will be submitted to our bank, American Express, and Discover Business Services to request merchant numbers. For assistance or questions regarding this form, please contact {INSERT PCI COMPLIANCE OFFICER'S NAME, PHONE & EMAIL}.

Best Practices for Offices Accepting Payments Cards

We understand that complying with the PCI DSS may be difficult and confusing for some departments. If you have identified a business need that requires you to accept credit and/or debit card payments, we recommend that you review this set of high-level best practices before you complete this application.

1. If you don't need it, don't store it!

• Many offices retain cardholder data (CHD) "just because." If you keep the transaction number and date, you can always ask the acquiring bank for the CHD if you need it.

• This includes paper and forms. Once the transaction has been processed, destroy the CHD on the form. This may require a redesign of the form to move the CHD to the bottom where it can be properly removed and cross-cut shredded.

2. Proper destruction

- All forms or paper with CHD should be shredded in a “cross-cut” type shredder.

- Third-party shredding services may be used, providing the bins that they provide are secure and cannot be removed from the area. Tracking chain of custody with the CHD and receiving a certificate of secure destruction is also recommended.

3. Online Payment Card Systems

- Many departments employ the use of third-party payment systems to outsource card processing to an online process. Many times it is considered good customer service to take phone calls, emails or some other form of communication to process a credit card transaction.

a. Never accept cardholder data that is sent via email; refer to the Payment Policy for the approved method of response for this type of situation.

b. It is not recommended to act as the customer and input their data for them. It would be better to verbally walk them through the flow as they enter in their data on the website themselves.

c. If you choose to accept payment data over the telephone, transactions should be conducted on a separate (isolated) computer or via a dial-up payment terminal.

4. Maintain clean desk policy

- CHD should not be left out on desks or in open areas when not needed. Even if leaving the desk for a short period, staff should keep material in a folder and lock the folder in the desk when they leave temporarily. At the end of the day, all CHD should be stored in a secure file cabinet or safe.

5. Electronic storage of CHD

- Do not copy or type CHD into spreadsheets or documents on general use workstations even for temporary use. Even if you don’t save the document, an image or file of the data is stored on the hard drive.

6. Never email Credit Card information

- Staff should never use email as a manner of transmitting Cardholder data

- Should a customer email their credit card information:

a. Reply to the sender, deleting the credit card information from the reply and inform them that “for their protection and California State University Bakersfield’s, policies dictate that credit card information shall not be accepted via email. Please use one of our accepted methods of processing your information: (in-person, online, fax, form, etc.).”

7. Do not allow unauthorized persons unaccompanied access to areas where credit card data is stored or processed

- This includes other California State University Bakersfield staff. As an example, maintenance and janitorial staff should not be permitted in secure areas unaccompanied. This sometimes requires a change in service times.

8. Document Desk Procedures

- To insure continuity when office personnel are out, have all individuals document their daily procedures for their role in the handling of confidential data. Include such items as receipt and processing procedures, disposition and destruction of CHD, and storage and transfer of forms within the office.

1. DEPARTMENT INFORMATION:

DEPARTMENT NAME: ______________________________

MERCHANT (LOCATION) NAME: ______________________________

Note: The merchant (location) name will appear on your customer's monthly statements and on the bank statements sent to the Controller's Office

INTERNET ADDRESS: ______________________________

Note: The merchant (location) name will appear on your customer's monthly statements and on the bank statements sent to the Controller's Office

MERCHANT (LOCATION) ADDRESS: ______________________________

Note: Merchant address must include Building & Room number. Statements will be mailed to this address.

2. PRIMARY CONTACT INFORMATION:

CONTACT NAME: ____________________ MAIN TELEPHONE #: ____________________

CONTACT TITLE: ____________________ ALT. TELEPHONE #: ____________________

EMAIL ADDRESS: ____________________ FAX NUMBER: ____________________

Note: Primary contact will be responsible for the overall process of accepting payment cards at this location and must be a full time employee. (Work Study employees are not allowed).

3. MERCHANT INFORMATION:

GIVE A BRIEF DESCRIPTION OF YOUR PAYMENT CARD BUSINESS:

(What is the main purpose of this merchant account? For example, registration fees, tuition for non-credit courses, tickets for events)

DATE SUBMITTED: ____________________ DESIRED "LIVE" DATE: ____________________

TRANSACTION TYPE TO BE ACCEPTED (Mark with an X):

( ) VISA ( ) AMERICAN EXPRESS ( ) DEBIT
( ) MASTERCARD ( ) DISCOVER

ESTIMATED ANNUAL CREDIT CARD VOLUME:

Total Annual Dollar Amount: $ ______
Average Amount per Transaction: $ ______
Annual Number of transactions: ______

DEPARTMENT ACCEPTS PAYMENT CARDS (Check all that apply):

( ) IN PERSON
( ) BY PHONE
( ) BY MAIL
( ) BY FAX
( ) ONLINE VIA UNIVERSITY'S APPROVED INTERNET PROCESSOR (name of provider)
( ) ONLINE VIA OTHER, NAME: ______

PROCESSING SYSTEMS (Check the types of system currently being used or will be used):

( ) POS Terminals ( ) Internet (Online) ( ) Other
If Other, describe in detail: ______
Current Third Party Vendor, if applicable: ______

CHARGEBACK INFORMATION:

Mail "Chargebacks" to (Provide name, title, and address including building and room #)

CONTACT NAME: ______ ADDRESS: ______
CONTACT TITLE: ______ ______

Note: Chargebacks are created when a customer disputes a charge. If action is not taken by the merchant within the time frame indicated on the letter, California State University Bakersfield will be charged by the payment card company. A journal entry must be made by the merchant to record such chargeback. If assistance with Chargebacks is needed, please call {ACCOUNTING OR CONTROLLER'S OFFICE CONTACT}.

IF PROCESSING USING A POINT OF SALE (POS) ELECTRONIC TERMINAL, PLEASE PROVIDE:

MODEL	FIRMWARE/SOFTWARE VER.	SERIAL NUMBER

IF PROCESSING OVER THE INTERNET, PLEASE PROVIDE:

TECHNICAL
CONTACT: ______ TELEPHONE #: ______

TITLE: ______________________ EMAIL ADDRESS: ______________________

FOR PROCESSING JOURNALS, PLEASE PROVIDE:

NAME: ______________________ TELEPHONE #: ______________________
TITLE: ______________________ EMAIL ADDRESS: ______________________

FOR PROCESSING CHARGEBACKS, PLEASE PROVIDE:

NAME: ______________________ TELEPHONE #: ______________________
TITLE: ______________________ EMAIL ADDRESS: ______________________

4. PROCESSING INFORMATION

1. Have you, or your employees, received training on how to handle cardholder data in a compliant manner?
   YES ( ) NO ( ) If NO, please explain ______________________

2. Do you, or your employees, have written instructions on how handle cardholder data in a compliant manner?
   YES ( ) NO ( ) If NO, please explain ______________________

3. Do you cross-cut shred documents that contain sensitive payment card information immediately after the transaction is processed?
   YES ( ) NO ( ) If NO, please explain ______________________

4. Are payment card numbers truncated on the receipt?
   YES ( ) NO ( ) If NO, please explain ______________________

5. Is the {technology used} kept in a secured and restricted area, away from public access?
   YES ( ) NO ( ) If NO, please explain ______________________

6. Is {technology used} inspected on a regular, periodic basis for tampering and/or substitution?
   YES ( ) NO ( ) If NO, please explain ______________________

7. Is a "unique code" assigned to each person with access to payment card processing and is this code not shared with another person?
   YES ( ) NO ( ) If NO, please explain ______________________

8. Is the {technology used} connected to an analog line?
   YES ( ) NO ( ) If NO, please explain ______________________

9. If accepting payment card information by fax, is the fax machine in a secured area and are the faxed documents destroyed immediately after the transaction is processed?
YES ( ) NO ( ) If NO, please explain ______________________________

10. If accepting payment card information by fax, is the fax machine a standalone device connected only to an analog phone line?
YES ( ) NO ( ) If NO, please explain ______________________________

11. Are California State University Bakersfield's *"Payment Card Processing Procedures"* being followed by employees involved in payment card handling?
YES ( ) NO ( ) If NO, please explain ______________________________

12. Do you educate employees on practices for accepting and processing payment cards and closing out batches?
YES ( ) NO ( ) If NO, please explain ______________________________

13. Do you, or your employees, audit transactions and settle batches daily?
YES ( ) NO ( ) If NO, please explain ______________________________

14. Do you have a back-up to process transactions daily in your absence?
YES ( ) NO ( ) If NO, please explain ______________________________

15. Do you, or your employees, take every measure possible to prevent duplicate entries?
YES ( ) NO ( ) If NO, please explain ______________________________

16. Have employees responsible for processing journals received payment card journal training?
YES ( ) NO ( ) If NO, please explain ______________________________

17. Do you educate employees on common types of payment card fraud and how to counteract them?
YES ( ) NO ( ) If NO, please explain ______________________________

18. Do you educate employees on common types of merchant mistakes and how to avoid them?
YES ( ) NO ( ) If NO, please explain ______________________________

19. Do you require background checks for employees involved in payment card processing, or employees that have access to such data?
YES ( ) NO ( ) If NO, please explain ______________________________

20. Do you require employees to acknowledge, at least annually, that they have read, understood, and agreed to abide by the California State University Bakersfield's policies and procedures on payment card processing by completing the Employee Statement of Understanding {link}?
YES ( ) NO ( ) If NO, please explain ______________________________

21. Do you have the ability to process payment cards if normal modes of processing are down?
YES ( ) NO ( ) If NO, please explain ______________________________

22. Do you limit the number of employees who process payment cards to appropriate employees based on their job duties?
YES ( ) NO ( ) If NO, please explain ______________________________

23. Do you keep the {Appropriate Department} aware of any changes in your payment card program?
YES ( ) NO ( ) If NO, please explain ______________________________

24. Is access to stored cardholder data restricted to users on a need to know basis?
YES ( ) NO ( ) If NO, please explain ______________________________

25. When an employee leaves the Department, is his/her access to payment card processing immediately revoked?
YES ( ) NO ( ) If NO, please explain ______________________________

26. Do you prohibit storage of cardholder data and other sensitive information?
YES ( ) NO ( ) If NO, please explain ______________________________

27. Do you prohibit storage of the full contents of any track from the magnetic stripe (on the back of the card) in a database, log files, or point of sale products?
YES ( ) NO ( ) If NO, please explain ______________________________

28. Do you prohibit storage of the card validation code (3 digit value printed on the signature panel of a card) in a database, log files, or point of sale products?
YES ( ) NO ( ) If NO, please explain ______________________________

29. Do you prohibit the transmission of CHD via insecure mediums, e.g. email or chat?
YES ( ) NO ( ) If NO, please explain ______________________________

30. Do you update the "Privacy Policy" to reflect changes and keep it current?
YES ( ) NO ( ) If NO, please explain ______________________________

31. Do you update the "Refund Policy" to reflect changes and keep it current?
YES ( ) NO ( ) If NO, please explain ______________________________

5. TECHNICAL INFORMATION:

1. Are all staff members who process payment cards aware of the "Emergency Contact Plan" in case the system has been breached or compromised?
YES ( ) NO ( ) If NO, please explain ______________________________

2. Do you train all staff members and test the Emergency Contact Plan, at least annually? (same as #1)
   YES ( ) NO ( ) If NO, please explain ____________________

3. Are default security settings, accounts, and passwords changed on production systems before taking the system into production?
   YES ( ) NO ( ) If NO, please explain ____________________

4. Is transmission of cardholder data and other sensitive information across public networks encrypted using PCI-approved methods?
   YES ( ) NO ( ) If NO, please explain ____________________

5. On all systems that are commonly affected by malware, is anti-malware software installed on all servers and workstations involved in payment processing , and is itregularly updated?
   YES ( ) NO ( ) If NO, please explain ____________________

6. THIRD PARTY PROCESSORS OR GATEWAYS INFORMATION:

If you are not using a Third Party Processor or Gateway, please go to PART 7.

1. Is a list of service providers (vendors) maintained including a description of the service(s) provided?
   YES ( ) NO ( ) If NO, please explain ____________________

2. Do you have a written agreement with an acknowledgment that indicates that the service provider (vendor) is responsible for the security of cardholder data?
   YES ( ) NO ( ) If NO, please explain ____________________

3. Has the written agreement been reviewed and approved by our Legal Department?
   YES ( ) NO ( ) If NO, please explain ____________________

4. Has the written agreement been reviewed and approved by Information Technology?
   YES ( ) NO ( ) If NO, please explain ____________________

5. Do you have a program in place to validate the service provider's (vendor's) PCI DSS compliance status before engaging in a new relationship?
   YES ( ) NO ( ) If NO, please explain ____________________

6. Do you have a program in place to validate the service provider's (vendor's) PCI DSS compliance on at least an annual basis?
   YES ( ) NO ( ) If NO, please explain ____________________

7. Is information maintained about which PCI DSS requirements are managed by the service provider (vendor), and which are managed by the merchant?

   YES ( ) NO ( ) If NO, please explain ______________________________

7. EMPLOYEE ATTESTATION STATEMENT

I attest that the information in this merchant questionnaire has been completed to the best of my knowledge and belief. I understand the intent of this merchant questionnaire and that the information I have provided is an important element of California State University Bakersfield's Payment Card Handling Policy {link}.

I attest that I have read California State University Bakersfield's policies, procedures and guidelines listed under the "Related Information" section of the California State University Bakersfield Payment Card Handling Policy.

I understand that payment card processing information is to be kept in the strictest of confidence to protect cardholder information and that failure to comply with California State University Bakersfield's Payment Card Handling Policy may result in disciplinary action, up to and including termination.

I confirm that I have read, understood, and agree to abide by the policies and procedures associated with accepting and handling payment cards on behalf of California State University Bakersfield.

Authorized Signature:	______________________________	*Date:*	______________
Printed Name:	______________________________	*Telephone #:*	______________
Title:	______________________________	California State University Bakersfield *ID:*	______________