CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

Payment Card Industry Policy

CSU Bakersfield Policy

Document Number:	ITS-90.029	**Last Revision Date:**	
Responsible Office:	Information Technology Services	**Effective Date:**	5/1/2023
Primary Author:	CIO & AVP of Information Technology		

General Description

Purpose:

This document and additional supporting documents represent California State University Bakersfield's policy to prevent loss or disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and the institution.

Definition:

Payment Card Industry Data Security Standard (**PCI DSS**) - The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/ organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org).

To accept credit card payments, California State University, Bakersfield must prove and maintain compliance with the Payment Card Industry Data Security Standards. The California State University, Bakersfield's Payment Card Policy and additional supporting documents provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions. This is done to reduce the institutional risk associated with the administration of credit card payments by individual departments and to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Visa Cardholder Information Security Plan (CISP) - Visa Inc. instituted the Cardholder Information Security Program (CISP) in June 2001. CISP is intended to protect Visa cardholder data - wherever it resides - ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into the Payment Card Industry Data Security Standard (PCI DSS).

MasterCard Site Data Protection Program (SDP) - The SDP Program, with the PCI DSS as its foundation, details the data security and compliance validation requirements in place to protect stored and transmitted MasterCard payment account data.

Scope:

The California State University, Bakersfield Payment Cards Policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of California State University, Bakersfield.

Policy/Procedure

It is the policy of California State University, Bakersfield to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the Financial Services Department. California State University, Bakersfield requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this policy document, the California State University, Bakersfield payment card procedures, and other supporting documents.

All entities of California State University, Bakersfield and related Auxiliaries that receive or expect to receive payments electronically must comply with the guidelines and procedures issued by the Financial Services Department. All entities who wish to take payments via payment cards must be approved by the CSUB PCI Committee. Once approved, the request should be forwarded to the Financial Services Department for final approval and implementation. All merchants should submit their requests for approval to the appropriate Vice President and then, once approved, forward the signed form to the Financial Services Department.

Entities accepting payment cards will sign an agreement with the Financial Services Department that details their responsibilities, as well as the security requirements (Payment Card Industry Data Security Standard and institutional Data Security Policies) that must be followed. This agreement may be updated from time to time as requirements change. Failure to follow the requirements of the agreement may result in the revocation of your ability to accept card payments.

Entities must accept only payment cards authorized by the Financial Services Department and agree to operate in accordance with the contract(s) the California State University, Bakersfield holds with its Service Provider(s) and the Card Brands. This is to ensure that all transactions are in compliance with the Payment Card Industry Data Security Standards (PCI DSS), Federal Regulations, NACHA rules, service provider contracts, and California State University, Bakersfield policies regarding security and privacy that pertain to electronic transactions.

Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

· Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements.
· Data that is not absolutely necessary in order to conduct business will not be retained in any format. All data will be treated as confidential.
· Specific retention requirements for cardholder data.
· Processes for secure deletion of data when no longer needed.
· A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.
· Physical access to data records is restricted to staff with a need to know.

All campus merchants are required to complete an annual PCI Self-Assessment Questionnaire (PCI SAQ) to the Information Technology Services Security team along with the merchant specific payment card handling procedures for review.

Cardholder data (CHD) received via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is never to be used to process a payment. Follow approved departmental procedures for the appropriate method of responding to and securely destroying the cardholder data.

All processing equipment is to be obtained via the Financial Services Department.
Exceptions to this policy will be limited and will require a business plan (including reason why the available central processing systems will not work for your area) to be submitted and approved by the Financial Services Department in advance of any equipment or system purchase.

All payments received must be deposited into a California State University, Bakersfield Approved Bank Account. The type and nature of the electronic transaction (e.g., ACH, Credit Card, Point of Purchase, wire, etc.) will dictate where the transaction will be deposited.

Accounting entries to record the receipt of the payment will be linked directly into the institution's Financial Information System (FIS), whenever possible, to ensure timely recording of transactions and expedite the prompt reconcilement of general ledger and bank accounts.

Attachments

PCI Best Practices

Administration and Department Payment Card Procedures

Application for New Payent Card Merchants

Review (Frequency and Process)

This policy shall be reviewed every two years by the Associate Vice President & CIO or a designate and provided to the Vice President of Business and Administrative Services for approval and then to Cabinet for final approval.