Administration and Department Payment Card Procedures
Last Revision Date: 2/22/2023

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:

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.

Procedures:

In the course of doing business at California State University Bakersfield, including affiliated organizations, it may be necessary for a department or other unit to accept payment cards. California State University Bakersfield requires all departments that accept payment cards to do so only in accordance with PCI DSS and the following procedures.

1. Card Acceptance and Handling

The opening of a new merchant account for the purpose of accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of the payment card in that department will be charged to the individual merchant.

1.1. Interested departments or merchants should contact (the payment coordinator) to begin the process of accepting payment cards. Steps include:

1.1.1. Completion of an "Application to become a Merchant Department"

1.1.2. Completion of training

1.1.3. Review and acknowledgement of the "Policies for Payment card Processing and Security", including proof of ongoing compliance with all requirements of the policy

1.1.4. If applicable, submit application for E-commerce for approval by the E-commerce committee. The application and policy are found at (location link).

1.2. Any department accepting payment cards on behalf of the institution or related foundation must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the primary is unavailable.

1.3. Specific details regarding processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the Financial Services Department.

1.4. All service providers and third-party vendors providing payment card services must be PCI DSS compliant. Departments who contract with third-party service providers must maintain a list that documents all service providers and:

1.4.1. Ensure contracts include language stating that the service provider or third-party vendor is PCI complaint and will protect all cardholder data.

1.4.2. Annually audit the PCI compliance status of all service providers and third-party vendors. A lapse in PCI compliance could result in the termination of the relationship.

2. Payment Card Data Security

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

PROCESSING AND COLLECTION

2.1. Access to cardholder data (CHD) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD and review the list periodically to ensure that the list reflects the most current access needed and granted.

2.2. Equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:

2.2.1. Maintaining an inventory/list of devices and their location.

2.2.2. Periodically inspecting the devices to check for tampering or substitution.

2.2.3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.

2.2.4 California State University Bakersfield does not maintain any PCI compliant networks or systems. Therefore, only Point to Point Encrypted (P2PE) credit card payment terminal devices are allowed to process transactions.

2.3. Email must never be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined below is critical. If payment card data is received in an email, then:

2.3.1. The email should be replied to immediately with the payment card number deleted stating that "California State University Bakersfield does not accept payment card data via email as it is not a secure method of transmitting cardholder data".

2.3.2. Provide a list of the alternate, compliant option(s) for payment.

2.3.3. Delete the email from your inbox and also delete it from your email Trash.

2.4. Fax machines used to transmit payment card information to a merchant department must be standalone machines with appropriate physical security; receipt or transmission of payment card data using a multi-function fax machine is not permitted.

2.5. Campus telephones connected to the analog or VOIP PBX systems must never be used to transmit payment card or personal payment information, nor should they be accepted as a method to supply such information. If it does occur notify the caller: “California State University Bakersfield does not accept payment card data via this telephone system as it is not a secure method of transmitting cardholder data. Please allow me to call you back from a secure line to complete this transaction”

2.5.1 Only dedicated cellular phones may be used to transmit payment card information.

2.5.2 PCI approved telephone devices can be obtained by contacting Telecom.

STORAGE AND DESTRUCTION

2.5. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.

2.6. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data.

2.7. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card validation code.

2.8. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

2.9. Cardholder data should not be retained any longer than that defined by a legitimate business need. CHD must be destroyed immediately following the required retention period using a PCI DSS-approved method of destruction. The INSTITUTION-

defined maximum period of time the data may be retained is (XX months). A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the required retention period.

3. Risk Assessment

Implement a formal risk assessment process in which current threats and vulnerabilities to the institution's network and processing environment, including staff, are analyzed. Risk assessments must be conducted annually. Information Technology should conduct the risk assessment of the infrastructure and threats; departments that accept payment cards should also conduct an assessment of their physical environments and assess risks to the payment environment. Address all threats with mitigation tasks, timelines and/or acceptance statements. Prepare and maintain documented output from the risk assessment exercise(s).

4. Incident Response

In the event of a breach or suspected breach of security, the department or unit must immediately execute the California State University Bakersfield Payment Card Incident Response Plan (include website or location here). The plan must include notifications, staff requirements, and handling procedures. If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify ITS Security. The Incident Response Plan should be reviewed and tested at least annually.

5. Policy and Training

Ensure policy and procedure documentation governing cardholder data exists and that it covers the entirety of the PCI DSS. Document users' acknowledgement of understanding and compliance with all policies and procedures annually. Ensure training on the PCI DSS and overall information security is provided to all staff members with access to cardholder data and/or the processing environment upon hire, and at least annually thereafter.

6. Sanctions

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation the payment card brands may assess penalties to the Institution's bank which will likely then be passed on to the Institution. Any fines and assessments imposed will be the responsibility of the impacted merchant. A one-time penalty of up to $500,000 per card brand per breach can be assessed as well as on-going monthly penalties.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state, or

federal laws. The California State University Bakersfield will carry out its responsibility to report such violations to the appropriate authorities.