CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

Electronic Commerce Services Standard

CSUSB, Information Technology Services

Last Revised: 10/20/2022 FINAL

REVISION CONTROL

Document Title: CSUSB – Electronic Commerce Services Standards

Author: Javier Torner, Laura Carrizales

Date	By	Action	Pages
11/7/2012	J. Torner L. Carrizales	Revision	All
6/27/2017	M. Lymuel	Updated entire document	All
7/18/2017	L. Carrizales	Formatted document	All
10/20/2022	G Au	Updated entire document	All

Review/Approval History

Date		By	Action	Pages
				All

Table of Contents

1.0 Purpose

The purpose of this security standard is to ensure that payment card activities comply with all applicable regulations and standards, such as the Payment Card Industry Data Security Standard (PCI-DSS) and are consistent with the appropriate university and CSU financial policies and procedures.

This standard defines the procedures to ensure that campus processes and procedures for handling payment card transactions are consistent, efficient and secure to protect the interests of the University and its end users.

This standard applies to ALL types of payment card activities transacted in-person, over the phone, via fax, mail or the Internet.

2.0Scope

This standard applies to all University departments, administrative areas, auxiliary units, contractors, consultants or agents who in the course of doing business on behalf of the University, accept, process, transmit, or otherwise handle cardholder information in physical or electronic format, regardless of whether revenue is deposited in a University or campus auxiliaries account.

3.0Governance

Every campus entity (Merchant Department), within scope of this standard, accepting payment cards and/or electronic payments on behalf of the University for goods, services, or donations must designate a management employee, referred as the Department Responsible Person (DRP), within that entity who will have primary authority and responsibility for the following:

1. Oversee payment card and eCommerce transaction processing within that Merchant Department
2. Ensure compliance with all applicable laws, regulations, policies, and standards.
3. Execute on behalf of the relevant Merchant Department, Payment Card Account Acquisition or Change Procedures.
4. Conduct annually the necessary risk assessments and questionnaires as required by the Payment Card Industry Data Security Standard (PCI-DSS) and address compliance gaps within the time period specified within current regulatory standards. Submit a copy of the appropriate self-assessment, gap analysis and attestation of compliance through the established campus procedures.

Office of Compliance Initiatives shall

1. Review self-assessments annually
2. In consultation with the Merchant Department and the Information Security Office, identify compliance gaps and assist the Merchant Department with corrections and mitigations.
3. Inform Student Financial Services Office for any non-compliance of staff training
4. Inform Student Financial Services of Merchant Department annual attestation.

Student Financial Services Office shall

1. Maintain a list of Merchant Departments on campus

2. Inform the Office of Compliance Initiative and the Information Security Office of any new Merchant Departments, or changes to a Merchant Department's merchant level or merchant type.
3. Review and approve any new requests to conduct eCommerce activities.
4. Revoke any authorization to conduct eCommerce activity for non-compliant Merchant Department.

Information Security Office shall

1. Assess and determine information security requirements for Merchant Departments.
2. Respond to incidents related to loss of cardholder data.
3. Oversee payment card information security program with the Office of Compliance Initiatives and Student Financial Services
4. Review compliance reporting with IT Governance (ISET) Sub-Committee annually and update procedures and standards accordingly

4.0Data Security Standards

Compliance with eCommerce standards requires that each campus entity conducting eCommerce activities should implement the following procedure:

Ensure that all employees (including the DRP), contractors and agents with access to payment card data within the Merchant Department acknowledge on an annual basis and in writing that they have read and understood this standard. These acknowledgments should be submitted, as requested, to the Vice President of Administration and Finance.

Ensure that all payment card data collected by the relevant Merchant Department in the course of performing University business, regardless of whether the data is stored physically or electronically, is secured and protected.

Data are considered to be secured only if all of the following criteria are met:

1. Only those with a need-to-know are granted access to payment card and electronic payment data.
2. Email, or any other form of electronic communication, should not be used to transmit payment card or personal payment information. If it should be necessary to transmit payment card information via email only the last four digits of the payment card number can be displayed.
3. Payment card or personal information is never downloaded onto any portable devices or media such as USB flash drives, compact disks, laptop computers or mobile devices.
4. Fax transmissions (both sending and receiving) of payment card and electronic payment information occurs using only fax machines which are attended by those individuals who must have contact with payment card data to do their jobs.
5. The processing and storage of personally identifiable payment card information on University computers and servers is prohibited.
6. Only secure communication protocols and/or encrypted connections to the authorized vendor are used during the processing of eCommerce transactions.
7. The three- or four-digit validation code printed on the payment card is never stored in any form; The full contents of any track data from the magnetic stripe are never stored in any form.
8. The personal identification number (PIN) or encrypted PIN block are never stored in any form; The primary account number (PAN) is rendered unreadable anywhere it is stored.
9. All but the last four digits of any credit card account number are masked when it is necessary to display credit card data;
10. All media containing payment card or personal payment data is retained no longer than a maximum of six (6) months and then destroyed or rendered unreadable

5.0 Incident Response

In the event of a suspected or confirmed loss of cardholder data, the DRP must immediately notify the VP for Administration and Finance and the campus Chief Information Security Officer. Details of any suspected or confirmed breach should not be disclosed in any email correspondence or to any third party without the consent of the VP of Administration and Finance. After normal business hours, notification shall be made to the University Police.

6.0Procedure

-

Campus entities interested in conducting eCommerce activities should first complete a Request to Establish/Maintain Cashiering Collection Point form with Student Financial Services. Failure to follow the established campus procedure may result in the denial of fund deposits and may result in the return of all funds collected by the department prior to approval.

Campus entities should not use or negotiate individual contracts with payment card companies or processors without approval from the Director of Accounting.

The Student Financial Services Office will provide entities with the information and requirements to use university adopted credit card processor(s) and applications.

The Student Financial Services Office will forward the necessary information to the Information Security Office to assess and determine the information security requirements for compliance with this standard.

An entity is not allowed to conduct eCommerce activities until it has been verified by the campus auditor that the eCommerce proposal meets all the university compliance requirements.

7.0Non-Compliance

Failure to comply with the security recommendation on this standard, including failure to promptly correct any identified compliance issues or submit the yearly self-assessment may result in revocation of the authorization to conduct eCommerce activities on behalf of CSUSB.