



CSUSB Electronic Commerce Services Standards
CSUSB, Information Security Office

Last Revised: 07/18/2017

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

Review/Approval History

Date		By	Action	Pages
				All

Table of Contents

1.0 Purpose	4
2.0 Scope	4
3.0 Responsibilities	4
4.0 Data Security Standards	4
5.0 Incident Response	5
6.0 Procedure	6
7.0 Non Compliance	6

1.0 Purpose

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

This standard defines the procedures to ensure that campus process and procedures for handling credit 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 credit card activity transacted in-person, over the phone, via fax, mail or the Internet.

2.0 Scope

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.

3.0 Responsibilities

Every campus entity, within scope of this standard, which is accepting payment cards and/or electronic payments on behalf of the University for goods or services (Merchant Department) 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:

Payment card and eCommerce transaction processing within that Merchant Department

Ensure compliance with all applicable laws, regulations, polices and standards.

Execute on behalf of the relevant Merchant Department, Payment Card Account Acquisition or Change Procedures.

Conduct annually the necessary risk assessments and questionnaires as required by the Payment Card Industry Data Security Standard (PCI-DSS) including:

Address compliance gaps and other PCI requirements appropriate to merchant department PCI compliance level

Complete Attestation of Compliance for PCI-DSS

Submit a copy of the appropriate Self-Assessment, gap analysis and attestation of compliance to the Information Security Office.

4.0 Data Security Standards

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

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

Only those with a need-to-know are granted access to payment card and electronic payment data;

Email, or any other form of electronic communication, should not be used to transmit credit card or personal payment information. If it should be necessary to transmit credit card information via email only the last four digits of the credit card number can be displayed.

Credit card or personal information is never downloaded onto any portable devices or media such as USB flash drives, compact disks, laptop computers or personal digital assistants.

Fax transmissions (both sending and receiving) of credit 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;

The processing and storage of personally identifiable credit card or payment information on University computers and servers is prohibited.

Only secure communication protocols and/or encrypted connections to the authorized vendor are used during the processing of eCommerce transactions;

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;

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;

All but the last four digits of any credit card account number are masked when it is necessary to display credit card data;

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 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.

6.0 Procedure

Campus entities interested in conducting eCommerce activities should first-complete a Request to Establish/Maintain Cashiering Collection Point form.

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 the 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.

7.0 Non 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 in behalf of CSUSB.