**eCommerce Policy**

**Effective Date:** 1/1/2014

**Definition**

This policy is intended to ensure that payment card and eCommerce activities are consistent, efficient and secure to protect the interests of the University and its customers. This policy applies to all types of payment card activity transacted in-person, over the phone, via fax, mail or the Internet. This policy provides guidance to ensure that payment card acceptance and eCommerce processes comply with the Payment Card Industry Data Security Standards (PCI DSS) and are appropriately integrated with the University’s financial and other systems.

**Authority**

CSUSM President

**Scope**

This policy applies to all persons, organizations and activities which, in the course of doing business on behalf of the University or Auxiliary, accept, process, transmit, or otherwise handle cardholder information in physical or electronic format.

![Signature]

Karen S. Haynes, President

![Date]

1/15/2014

Approval/Date

---

Revised:

Implemented initially: 1/1/2014
I. BACKGROUND

A. In response to increasing incidents of identity theft, the major payment card companies created the Payment Card Industry Data Security Standard (PCI DSS) to help prevent theft of customer data. PCI DSS applies to all businesses that accept payment cards to procure goods or services. Compliance with this Standard is enforced by the payment card companies and generally, non-compliance is discovered when an organization experiences a security breach which includes card member data.

B. Security breaches can result in serious consequences for the University, including release of confidential information, damage to reputation, the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept payment card and eCommerce payments.

II. RESPONSIBILITIES

A. Every college or administrative area accepting payment cards and/or electronic payments on behalf of the University for goods or services (Merchant Department) must designate a management employee within that organization who will have primary authority and responsibility for payment card and eCommerce transaction processing within that Merchant Department. This individual is referred to in the remainder of this policy as the Merchant Department Responsible Person (MDRP).

B. All MDRPs are responsible for:

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

2. Ensuring that all employees (including the MDRP), contractors and agents with access to payment card data within the relative Merchant Department acknowledge on an annual basis and in writing that they have read and understood this Policy. These acknowledgements should be submitted, as requested, to the Vice President of Finance & Administrative Services.

3. Ensuring that all payment card data collected by the relevant Merchant Department in the course of performing University business is secured, regardless of whether the data is stored physically or electronically. Data is considered to be secured only if all of the following criteria are met:

   a) Only those persons with “need-to-know” are granted access to payment card and electronic payment data;
b) Email may not be used to transmit payment card or personal payment information. If it should be necessary to transmit transaction information via email only the last four digits of the payment card number can be displayed.

c) Payment card or personal information is never downloaded onto any external site, portable devices or media such as USB flash drives, compact disks, laptop computers, or cloud storage systems;

d) Fax transmission (both sending and receiving) of payment card and electronic payment information occur using only fax machines which are attended by those individuals who must have contact with payment card data to do their jobs;

e) The processing and storage of personally identifiable payment card or payment information on campus computers and servers is prohibited.

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

g) The three or four digit validation code printed on the payment card is never stored in any form;

h) The full contents of any track data from the magnetic stripe are never stored in any form;

i) The personal identification number (PIN) or encrypted PIN block are never stored in any form;

j) The primary account number (PAN) is rendered unreadable anywhere it is stored;

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

l) 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.

C. Responding to a security incident.

1. In the event of a suspected or confirmed loss of cardholder data, the MDRP must immediately notify the campus Information Security Officer, iso@csusm.edu or 760-750-4787. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notification shall be made to the University Police, (760) 750-4567.
III. PAYMENT CARD ACCOUNT ACQUISITION OR CHANGE PROCEDURES

A. To acquire or change a payment card account, the MDRP or his/her designee must submit a Payment Card Account Application to the appropriate organization’s designated Administrative Services Manager (ASM)\(^1\). The application must be signed by the MDRP, the appropriate ASM and appropriate Associate Vice President or Dean. Applications for new eCommerce activities must also be signed by the Chief Information Officer. All eCommerce activities shall be processed by a third party vendor authorized by the University.

B. All requests shall be reviewed and approved by the appropriate ASM and the campus Information Security Officer. When an application to acquire a payment card account is approved, the ASM will assist the MDRP in establishing the new merchant account activity.

C. The MDRP may appeal a decision to deny an application to acquire or change a payment card account to the Vice President, Finance & Administrative Services.

IV. WIRELESS TECHNOLOGY

A. The University prohibits the use of campus wireless technology to process or transmit cardholder data unless explicitly authorized by the ISO. Requests for Payment Card Account Acquisition or Change which include the use of wireless technology will be reviewed on a case by case basis and the ISO shall carefully consider the need for the technology against the risks of a wireless payment environment.

B. Cellular wireless technology used to process payment cards must be provided by a vendor approved by the campus ISO. These systems must comply with the criteria identified in § 3(B)(3) above. Activation of network access equipment for vendors will be permitted only when necessary and be immediately deactivated after use.

V. POLICY MANAGEMENT

A. California State University San Marcos may modify this policy as required. All modifications shall be consistent with the current Payment Card Industry Data Security Standard.

B. Instructional & Information Technology Services (IITS) shall regularly monitor and test the University Network, coordinate the University’s compliance with the PCI Standard’s technical requirements and verify the security controls of systems authorized to process payment cards.

C. The Information Security Office shall monitor the changes in the PCI DSS and related requirements to ensure that this policy remains current and shall coordinate and lead any campus response to a security breach involving cardholder data.

\(^1\) Vice President for Finance & Administrative Services
D. The Information Security Office shall conduct the University PCI DSS Self-Assessment and complete the University’s Attestation of Compliance.

VI. SANCTIONS

A. The Chief Information Officer may suspend payment card account privileges of any college or administrative unit not in compliance with this policy. Any college or administrative unit engaged in payment card activities will be responsible for financial loss due to poor internal or inadequate controls or negligence in adhering to the PCI Data Security Standard.

B. Faculty, staff, and student employees who fail to comply with this policy may be subject to appropriate disciplinary and/or personnel action up to and including termination, consistent with University policies, rules, and collective bargaining agreements.

VII. DEFINITIONS

A. Cardholder: The customer to whom a payment card has been issued or the individual authorized to use the card.

B. Cardholder Data: All personally identifiable data about the cardholder (i.e., account number, expiration date, cardholder name, address, telephone number, social security number, etc.)

C. Card-Validation Code or Value: Refers to either (1) magnetic-stripe data or (2) printed security features. Data element on a card’s magnetic strip that uses a secure process to protect data integrity on the strip, and reveals any alteration or counterfeiting. The following list provides the terms for each card brand:

1. CAV – Card Authentication Value (JCB payment cards)
2. CVC – Card Validation Code (MasterCard payment cards)
3. CVV – Card Verification Value (Visa and Discover payment cards)
4. CSC – Card Security Code (American Express)

D. For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment card. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following provides an overview:

1. CID – Card Identification Number (American Express and Discover payment cards)
2. CAV2 – Card Authentication Value 2 (JCB payment cards)
3. CVC2 – Card Validation Code 2 (MasterCard payment cards)

4. CVV2 – Card Verification Value 2 (Visa payment cards)

E. Encryption: The process of converting information into an unintelligible form to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process against unauthorized disclosure.

F. Magnetic Stripe Data (Track Data): Data encoded in the magnetic stripe used for authorization during payment transaction.

G. Merchant: For the purposes of the PCI DSS and this policy, a merchant is defined as any university department or other entity that accepts payment cards bearing the logos of any for the five members of PCI SCC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

H. Payment Card: Any payment card/device that bears the logo of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.

I. Merchant Department Responsible Person (MDRP): A management employee within a department with primary authority and responsibility for payment card and eCommerce transaction processing within that Merchant Department.

J. Administrative Services Manager (ASM): A management employee with broad oversight responsibility for financial matters within the campus or auxiliary organization.

K. Payment Card Account Change

1. Any change in the payment account including, but not limited to:
   
a) the use of existing payment card accounts for new purposes;
   
b) the alteration of business processes that involve payment card processing activities;
   
c) the addition or alteration of payment systems;
   
d) the addition or alteration of relationships with third-party payment card service providers, and
   
e) the addition or alteration of payment card processing technologies or channels.

L. Payment Card Industry (PCI) Data Security Standard (DSS): A multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
VIII. TRAINING

A. Employees who are expected to be given access to cardholder data shall be required to complete upon hire and at least annually security awareness training focused on cardholder data security. Employees shall be required to acknowledge at least annually that they have received training, understand cardholder security requirements, and agree to comply with these requirements.