

Merchant or Merchant Department	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 of the five members of the Payment Card Industry Security Standards Council (American Express, Discover, JCB, MasterCard or VISA) as payment for goods and/or services, or to accept donations.
Merchant Department Responsible Person (MDRP)	A management employee within a department who has primary authority and responsibility for payment card and eCommerce transaction processing within that department.
Payment Card	Any payment card/device that bears the logo of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.
Payment Card Account Change	Any change in the payment account including, but not limited to: <ul style="list-style-type: none"> • the use of existing payment card accounts for new purposes; • the alteration of business processes that involve payment card processing activities; • the addition or alteration of payment systems; • the addition or alteration of relationships with third-party payment card service providers, and • the addition or alteration of payment card processing technologies or channels.
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.
Sensitive Authentication Data	Security-related information (card validation codes/values, full magnetic-stripe data, or personal identification number (PIN)) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.

IV. APPLICABILITY

This policy applies to all California State University, Long Beach (CSULB) employees, 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.

This policy applies to all University departments and administrative areas which accept payment cards regardless of whether revenue is deposited in a University or Auxiliary financial account.

V. ACCEPTABLE PAYMENT CARDS

California State University, Long Beach currently accepts VISA, MasterCard, Discover and American Express Card and has negotiated contracts for processing payment card transactions. Individual University units may not use or negotiate individual contracts with these or other payment card companies or processors. All individual University units must use the campus negotiated contracts.

VI. PROHIBITED PAYMENT CARD ACTIVITIES

California State University prohibits certain credit card activities that include, but are not limited to:

- accepting payment cards for cash advances
- discounting a good or service based on the method of payment
- adding a surcharge or additional fee to payment card transactions
- using a paper imprinting system unless approval is granted by Cashiering Services

VII. PAYMENT CARD FEES

Each payment card transaction will have an associated fee charged by the credit card company. Payment card fees will be allocated to the PeopleSoft general ledger account identified by the Merchant Department.

VIII. REFUNDS

When a good or service is purchased using a payment card and a refund is necessary, the refund must be credited back to the account that was originally charged. Refunds in excess of the original sale amount or cash refunds are prohibited.

IX. CHARGEBACKS

Occasionally a customer will dispute a payment card transaction, ultimately leading to a chargeback. In the case of a chargeback, the merchant department initiating the transaction is responsible for notifying the CSULB Cashiering Office and for providing appropriate supporting documentation.

X. MAINTAINING SECURITY

- Departments and administrative areas accepting payment cards on behalf of the University are subject to the Payment Card Industry Data Security Standards (PCI DSS).
- The University prohibits the transmission of cardholder data or sensitive authentication data via e-mail or unsealed envelopes through campus mail as these are not secure.
- The University requires that all external services providers that handle payment card information be PCI compliant.
- The University restricts access to cardholder data to those with a business “need to know.”
- For electronic media, cardholder data shall **not** be stored on servers, local hard drives, or external (removable) media including floppy discs, CDs or thumb (flash) drives unless encrypted and otherwise in full compliance with PCI DSS.
- For paper media, cardholder data shall not be stored unless approved for legitimate business purposes.

XI. RESPONSIBILITIES

Merchant Department Responsible Persons (MDRPs) are responsible for:

- Executing on behalf of the relevant Merchant Department, Payment Card Account Acquisition or Change Procedures.
- 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 University Manager, Student Account Services & Cashiering.
- Ensuring 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. 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 is not to 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 that 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; and
 - Notifying the University Director, Information Security Management and Compliance (562) 985-4818 in the event of suspected or confirmed loss of cardholder data. 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, (562) 985-4101.

Information Technology Services shall regularly monitor and test the University Network and coordinate the University’s compliance with the PCI Standard’s technical requirements and verify the security controls of systems authorized to process credit cards.

The Director, Information Security Management and Compliance shall maintain currency with the requirements of 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.

The Manager, Student Account Services and Cashiering shall:

- Provide training to ensure that university merchants are trained in accepting and processing payment cards in compliance with this policy;
- Work with external vendors and coordinate payment card policies, standards, and procedures;
- Serve as liaison between Financial Management Services, Information Technology Services, and the university merchant for Payment Card account acquisition or change procedures; and
- Review and modify the *Application for Payment Card Account Acquisition or Change* as necessary.

Internal Auditing Services shall:

- Periodically review university merchant compliance with this policy and the Payment Card Industry (PCI) Data Security Standards (DSS);
- Identify unapproved payment applications or external vendors that collect payment card data on behalf of the university and notify Cashiering Services; and
- When required, conduct the University PCI DSS Self-Assessment and complete the University's *Attestation of Compliance*.

XII. PAYMENT CARD ACCOUNT ACQUISITION OR CHANGE PROCEDURES

To acquire or change a payment card account, the MDRP or his/her designee must submit an *Application for Payment Card Account Acquisition or Change* to the University Cashiering Office at cashiers@csulb.edu. The application must be signed by the MDRP and appropriate Associate Vice President or Dean. Applications that request eCommerce activities must also be signed by the Associate Vice President, Information Technology Services. All eCommerce activities shall be processed by a third-party vendor authorized by the University.

All requests shall be reviewed by the Manager, Student Account Services & Cashiering, the Director of Information Security Management and Compliance and the Director, Network Services. The Manager, Student Account Services & Cashiering shall respond to all applications. When an application to acquire a payment card account is approved, the Manager, Student Account Services & Cashiering will assist the MDRP in establishing the new merchant account activity. All card processing terminals shall be obtained through Cashiering Services.

The MDRP may appeal a decision to deny an application to acquire or change a payment card account to the Associate Vice President, Financial Management.

Each auxiliary organization shall develop procedures for payment card account acquisition or change within their organization.

XIII. WIRELESS TECHNOLOGY

The University discourages the use of wireless technology to process or transmit cardholder data. Requests for Payment Card Account Acquisition or Change that include the use of wireless technology will be reviewed on a case by case basis and shall carefully consider the need for the technology against the risk of a non-secure payment environment.

If the use of wireless technology is approved, the storage of cardholder data on local hard drives, floppy disks or other external media is prohibited. It is also prohibited to use cut-and-paste and print functions during remote access. Activation of modems for vendors will be permitted only when no other alternative is available and will be immediately deactivated after use.

XIV. SANCTIONS

The Associate Vice President, Financial Services may suspend credit card account privileges of any department or administrative unit not in compliance with this policy or that places the University at risk.

Any department or administrative unit engaged in payment card activities will be responsible for any financial loss due to inadequate internal controls or negligence in adhering to the PCI Data Security Standard.

XV. TRAINING

Employees who are expected to be given access to cardholder data shall be required to complete upon hire, and at least annually thereafter, 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.

APPROVED JULY 2009



**MARY STEPHENS, VICE PRESIDENT
ADMINISTRATION & FINANCE**