# UPSILON ALPHA OMEGA CHAPTER

# ONLINE CREDIT CARD/PURCHASING POLICY

## I. PURPOSE

The purpose of this policy is to establish business processes and procedures for accepting payment cards online for Upsilon Alpha Omega Chapter (UAO) that will minimize risk and provide the greatest value, security of data, and availability of services to each chapter member within the rules and regulations established by the Payment Card Industry (PCI) and articulated in the PCI Data Security Standards (DSS). Additionally, these processes are intended to ensure that payment card acceptance procedures are appropriately integrated with Upsilon Alpha Omega's financial and other systems.

## II. DEFINITIONS

**Cardholder**

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

**Cardholder Data**

All personally identifiable data about the cardholder (i.e., account number, expiration date, cardholder name.)

**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.

**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 orVISA) 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:

- the use of existing payment card accounts for new purposes;
- the alternation of business processes that involve payment card processing activities;
- the addition or alteration of payment systems;
- the addition or alternation of relationships with third-party payment card service providers, and
- the addition or alternation of payment card processing technologies or channel

**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.

## III. ACCEPTABLE PAYMENT CARDS

UAO currently accepts VISA, MasterCard, Discover and American Express Card and has negotiated contracts for processing payment card transactions.

## IV. 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.

## V. 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.

## VI. MAINTAINING SECURITY

- UAO accepting payment cards on behalf of the chapter are subject to the Payment Card Industry Data Security Standards (PCI DSS).

- UAO prohibits the transmission of cardholder data or sensitive authentication data via email or unsealed envelopes through campus mail as these are not secure.
- UAO requires that all external services providers that handle payment card information be PCI compliant.
- UAO 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.

## VII. 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 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; and

## FURTHER INFORMATION

Upsilon Alpha Omega Chapter
info@upsilonalphaomega.com

**APPROVED JULY 2012**