CalPolyPomona

Philanthropic Foundation

POLICIES AND PROCEDURES

Subject: Policy for Accepting Payment (Credit) Card and Ecommerce Payments

Policy No. 511

Date: 07/01/2019

PURPOSE

The purpose of this policy is to establish business processes and procedures for accepting payment cards at Cal Poly Pomona Philanthropic Foundation (Foundation) that will minimize risk and provide the greatest value, security of data, and availability of services to each Foundation merchant account 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 the Foundation's financial and other systems.

BACKGROUND

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, noncompliance is discovered when an organization experiences a security breach that includes cardholder data. Security breaches can result in serious consequences for the Foundation, 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.

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).

Foundation Financial Services approves all third-party service providers and coordinates the policies and procedures for accepting payment cards at all Cal Poly Pomona Philanthropic Foundation venues.

Merchant or Merchant Department - For the purposes of the PCI DSS and this policy, a merchant is defined as any Foundation activity that accepts payment cards bearing the logos of any of the five members of the Payment Card Industry Security Standards Council (e.g., American Express, Discover, MasterCard or VISA) as payment for goods and/or services, or to accept donations.

Merchant Department Responsible Person (MDRP) - A MDRP is a Project Director or their designee who has primary authority and responsibility for payment card and ecommerce transaction processing activities within the designated project.

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

Payment Card Account Change - Any changes 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.

APPLICABILITY

This policy applies to all cardholders of the Cal Poly Pomona Philanthropic Foundation and contractors, consultants or agents who, in the course of doing business on behalf of the Foundation, accept, process, transmit, or otherwise handle cardholder information in physical or electronic format. This policy applies to all related departments and administrative areas, which accept payment cards regardless of whether the proceeds are deposited in a Foundation project.

ACCEPTABLE PAYMENT CARDS

Foundation currently accepts VISA, MasterCard, Discover and American Express Card and has negotiated contracts for processing payment card transactions. Foundation Project Directors or designee may not use or negotiate individual contracts with these or other payment card companies or processors. All Foundation Project Directors must use the Foundation-negotiated contracts.

PROHIBITED PAYMENT CARD ACTIVITIES

Foundation 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 unless advance approval is granted by the Foundation (e.g., tuition for non-credit course)
- Using a paper imprinting system

PAYMENT CARD FEES

Each payment card transaction will typically have an associated fee charged by the credit card company. Payment card fees will be allocated to the project identified by the Merchant Department.

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 credit card that was originally charged. Refunds in excess of the original sale amount or cash refunds are prohibited. Fees charged by the credit card company when the payment transaction is processed cannot be refunded.

CHARGEBACKS

Occasionally a customer will dispute a payment card transaction, ultimately leading to a chargeback. In the case of a chargeback, the Project Director initiating the transaction is responsible for notifying the Foundation for providing appropriate supporting documentation.

MAINTAINING SECURITY

- Project Directors accepting payment cards on behalf of the Foundation are subject to the Payment Card Industry Data Security Standards (PCI DSS).
- The Foundation prohibits the transmission of cardholder data or sensitive authentication data via email or unsealed envelopes through campus mail, as these are not secure.
- The Foundation requires that all external services providers that handle payment card information be PCI compliant.
- The Foundation 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 such as reconciliation. Otherwise, paper media should be cross- shredded immediately after completion of processing.

RESPONSIBILITIES

I. **Merchant Department Responsible Persons (MDRPs) Project Directors** are responsible for:

- Executing on behalf of the relevant Merchant Department, **Payment Card Account Acquisition or Change Procedures**.
- Ensuring that all cardholders 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.

- Ensuring that all payment card data collected by the relevant Merchant Department in the course of performing Foundation 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;
- 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's Information Security Officer 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.

Foundation operates within the University IT infrastructure and its network. Therefore, **University's Information Technology Services** is responsible to 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.

University's Information Security Officer will ensure this policy remains current and shall coordinate and lead any campus response to a security breach involving cardholder data related to Foundation's obligation for compliance with PCI DSS.

PAYMENT CARD ACCOUNT ACQUISITION OR CHANGE PROCEDURES

To acquire or change a payment card account, the MDRP Project Director or his/her designee must submit an Application for Payment Card Account Acquisition or Change which will be reviewed for approval by Chief Operating Officer All ecommerce activities shall be processed by a third party vendor authorized by the Foundation.

WIRELESS TECHNOLOGY

The Foundation allows the use of wireless technology to process or transmit cardholder data if fully encrypted point to point, and not run through the campus wireless network. 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 such that a secure payment environment is provided. 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.

SANCTIONS

The Foundation Chief Operating Officer (in consultation with the Foundation CEO) may suspend credit card account privileges of any project not in compliance with this policy or that places the Foundation at risk. Any project 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.

TRAINING

Anyone 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. All cardholders shall be required to acknowledge at least annually that they have received training, understand cardholder security requirements, and agree to comply with these requirements.