****

# Payment Card Industry (PCI) Data Security Program and Standard

## Implementation

|  |  |
| --- | --- |
| **Effective Date:** | 01/10/14 |
| **Review Frequency:** | Annual |
| **Responsible Officer:** | Director of Fiscal Services / University Controller |

## Revision History

|  |  |  |
| --- | --- | --- |
| **Date** | **Action** | **Pages** |
| 10/15/13 | Initial Draft developed based on Humboldt State and other university models (Thomas Bourne) | All |
| 11/01/13 | Reviewed and added reference to ICSUAM 3102.05 (Brett Holman) | All |
| 11/25/13 | Initial review by ISO and OCIO (Sharif Sharifi / Mary Shaffer) | All |
| 01/10/14 | Consolidated/reformatted as policy (for CAP) and PCI program/standard (Mary Shaffer) | All |

## Brief Description:

To ensure campus compliance with the Payment Card Industry Data Security Standard (PCI-DSS)

## Related Policy:

* [Cal Poly Information Security Program [PDF]](http://security.calpoly.edu/sites/security/files/docs/policy/isp.pdf)
* [Cal Poly Information Security Policy, Standards, Guidelines, Procedures, and Forms](http://security.calpoly.edu/content/policies/index)
* [CSU Debit/Credit Card Payment Policy (ICSUAM 3102.05)](http://www.calstate.edu/icsuam/sections/3000/3102.05.shtml)

## Introduction:

The purpose of this program is to ensure that payment card (credit card) and eCommerce activities are consistent, efficient, and secure to protect the interests of the University, its associated auxiliaries, and its customers. This standard provides guidance to ensure that campus credit card acceptance and eCommerce processes comply with the Payment Card Industry Data Security Standard (PCI DSS) and are appropriately integrated with the University’s financial and other systems.

## Scope:

This policy applies to California Polytechnic State University as well as its self-supporting operations, contractors, consultants, or agents who, in the course of doing business on behalf of the University, accept, process, transmit, store, or otherwise handle cardholder information in physical or electronic form. This policy also applies to all Cal Poly auxiliary organizations that accept process, transmit, store, or otherwise handle cardholder information in physical or electronic form. Additionally, this policy applies to all University departments and administrative areas that accept payment cards, regardless of whether revenue is deposited in a University or auxiliary account. This policy applies to all types of credit card activity transacted in person, over the phone, via fax, mail, or the internet.

## PCI Security Standards

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process, or transmit data, are mandatory for their respective stakeholders, and are enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and VISA Inc.

* PCI Data Security Standard: The PCI DSS applies to any entity that captures, stores, processes, or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. Any business activity that accepts or processes payment cards must comply with the PCI DSS.
* PCI Data Security Standard for Merchants and Processors:The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents steps that appeal to common sense and mirror best security practices.

### Operating Principles

The following operating principles must be used by departments when accepting credit card information in order to process payments for services, purchases, registration, etc.

* All merchant sites and merchant card processors must be authorized and approved by the Director of Student Financial Services**.**
* Such authorization is required for new credit card acceptance channels / merchant accounts, and any addition or change to an existing channel/account including, but not limited to, the:
	+ use of existing credit card acceptance channels / merchant accounts for new purposes
	+ alteration of business processes that involve payment card processing activities
	+ addition or alteration of payment systems or technologies
	+ addition or alterations of relationships with third-party payment card service providers
* Service Level Agreements must be developed between Contracts and Procurement and any department or entity processing credit cards.
* All merchant card services offered by the University must be delivered using software, systems, and procedures that are compliant with applicable standards.
* When processing credit card transactions, only the minimum amount of information necessary to verify the identity of the cardholder and the legitimacy of the cardholder authorization should be gathered. For example, manual requests to process a customer’s credit or debit card may contain the following elements:
	+ Properly signed/executed authorization from the cardholder (unless processing over the telephone as provided for in NACHA guidance on TEL transactions)
	+ Credit/debit card account number with expiration date
	+ The cardholder’s correct billing address
	+ Authorization codes (Card Identification Number), if the cardholder is not physically present

### Credit Card Merchant Numbers

* All credit card merchant ID numbers must be obtained from, or with the consent of Cal Poly Student Financial Services. Revenue-generating departments are prohibited from obtaining merchant ID numbers directly from the credit card companies or processors.
* Departments must use only campus-approved third-party providers to ensure PCI compliance.

### Credit Card Acceptance Channels

* Credit card information can be accepted through a Cal Poly authorized web application, an approved wireless device, by telephone, or in person only.
* Credit card information cannot be accepted via email and should never be emailed from the department. 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.
* Departments are not permitted to capture, transmit, process, or store credit card information on Cal Poly computer systems, fax machines, the internet, email, or any removable electronic storage device (USB memory stick, hard drive, zip drive, etc.), not even if encrypted, without written authorization of the Director of Student Financial Services.
* When possible, cashiering sites accepting credit card payments should only use Point of Sale terminals or equipment supplied to the location by the campus’ merchant card processor. In all cases, Point of Sale terminals and systems must be configured to prevent retention of the full magnetic strip, card validation code, PIN, or PIN Block cardholder data once a transaction has been authorized.
	+ The three- or four-digit validation code printed on the payment card, referred to as the Card Identification Number (CID), must never be stored in any form. The CID number may also be referred to as the CVC2 or CVV2.
	+ The full contents of any track data from the payment card’s magnetic stripe must never be stored in any form.
	+ The personal identification number (PIN) or encrypted PIN block must never be stored in any form.
	+ If electronic storage is authorized, the primary account number (PAN) must be rendered unreadable anywhere it is stored.
	+ All but the last four digits of any credit card account number must be masked when it is necessary to display credit card data.
	+ If electronic storage is authorized, credit card data must be encrypted at rest and in transit.
	+ If storage is authorized, all media containing payment card or personal payment data may be retained no longer than a maximum of 14 days, or when the information is no longer needed, whichever is earlier, and then must be destroyed or rendered unreadable.
	+ If storage is authorized, cardholder data must be encrypted at all times (i.e., at rest and during transmission).

### Credit Card Information Storage

* Paper records containing credit card data must be secured at all times, e.g., stored in a locked room or file cabinet. Access to the storage area(s) must be limited to authorized personnel only.

### Credit Card Receipts

* Credit card receipts that go to the customer may only show the last four digits of the credit card number. Also, the credit card expiration date should not appear on the receipt.
* Retain the original receipts, which show the last four digits of the credit card number, for all transactions and any original, signed documentation in a secure location for a maximum of 12 months as required by [Cal Poly’s Information Retention and Disposition Schedules](http://afd.calpoly.edu/acs/recordretention/retentionschedules.asp).

### Annual Self-Assessment and Network Scan

* Each department processing payment cards must complete an annual PCI DSS Compliance Internal Assessment Questionnaire. Once completed, the questionnaire should be made available for an annual on-site visit by representatives of the PCI DSS Compliance Steering Committee.
* Departments must work to resolve any exceptions to this policy discovered during the annual on-site visit. Departments must also work with the Information Security Officer to address any exceptions pertaining to technology or electronic storage.

### Imprint Machines

* The use of imprint machines is prohibited and any exception must be approved by the Director or Student Financial Services.

### Check Conversion to ACH (as required by ICSUAM)

* Checks received and converted into an ACH transaction, or telephone authorizations for payment shall be processed in conformance to the National Automated Clearinghouse Association (NACHA) Operating Rules and compliant to relevant state and federal rules and regulations.

### Prohibited Payment Card Activities:

* Prohibited credit card activities include, but are not limited to:
	+ accepting payment cards for cash advances
	+ discounting a good or service based on the method of payment
	+ using a paper imprinting system unless an exception is approved by the Director of Student Financial Services

### Training

* Employees who are expected to be given access to cardholder data shall initially be required to complete PCI DSS Introductory Training and then renew that training at least annually.
* 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.

## 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, e.g., Primary Account Number (PAN), cardholder name, billing address, expiration date

### Encryption

The process of converting information into an unintelligible form to anyone except holders of a specific cryptographic key (Use of encryption protects information that is between the encryption process and the decryption process from unauthorized disclosure.)

### Merchant or Merchant Department

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

### Payment Card

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

## Responsibilities:

### Student Financial Services

Student Financial Services has been delegated the authority by the campus CFO to approve all physical payment locations, websites, third party processors, or any channel accepting credit card payments, and will be responsible for verifying that credit card payments are only accepted at approved locations using approved merchant card processors. Additional Student Financial Services responsibilities include:

* Establishing and maintaining a process for campus departments to accept payment cards.
* Approving Credit Card Acceptance Channel Authorization Requests before payment cards can be accepted.
* Verifying that all service providers are listed on the List of PCI DSS Validated Service Providers (VISA’s website).
* Verifying the existence of a certification letter from a qualified security assessor.
* Verifying the existence of the service auditor’s report compiled under the Statement of Auditing Standards (SAS) #70.
* For all third-party payment software applications that capture, store, process, or transmit cardholder data as part of an authorization or settlement, verifying, on an annual basis, that the third-party software applications are compliant with applicable payment card requirements.
* Ensuring that each campus department that accepts payment cards completes the PCI DSS Compliance Internal Assessment Questionnaire required by applicable standards on an annual basis.
* Ensuring that each department receives an annual on-site visit to assess PCI DSS compliance.
* Maintaining a central file of all documentation indicating third-party vendor and third-party payment software application compliance with applicable requirements.
* Developing and maintaining the PCI DSS Introductory Training and related records of completion
* Authorizing PCI Network/Account access for employees who have completed PCI training
* Coordinating and leading any campus response to a security breach involving cardholder data
* Updating, maintaining and disseminating campus PCI standards and practices as needed
* Serving as chair of Cal Poly’s PCI DSS Steering Committee
* Working with the Information Security Coordinator and PCI DSS Steering Committee,
	+ Coordinate campus compliance with PCI DSS administrative and technical requirements and verify the security controls of systems authorized to process credit cards
	+ Ensure that PCI DSS Self-Assessments and Attestations of Compliance are completed in a timely manner in accordance with PCI DSS standards

### Merchant Department Responsible Person (MDRP)

Every department or administrative area accepting payment cards and/or electronic payments on behalf of the University for goods, services, or donations (the “merchant department”) must designate a Merchant Department Responsible Person (MDRP).

The MDRP must be a management employee with primary authority and responsibility for payment card and eCommerce transaction processing within that department. All 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 that they have read and understood this standard. These acknowledgements should be submitted, as requested, to the Student Financial Services office.
* 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 according to this standard.
* In the event of a suspected or confirmed loss of cardholder data, immediately notifying the Information Security Office and the Director of Student Financial Services. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notification shall be made to Cal Poly University Police at (805) 756-2281.

### Employees Handling Credit Card Information

* All employees handling cardholder data must have signed Responsible Use Policy and Confidentiality / Security Agreements on file.
* All employees handling cardholder data must have received initial PCI DSS compliance training within the previous one-year period.
* When employees have access to payment card data, whether accepted via telephone, in person, or through other non-electronic methods, the data must be secured before employees leave their workstations for any purpose.
* When payment card data must be physically transported, the means of physical transport must be secure. Credit card data should never be sent via interoffice mail.
* Payment card data on paper must be cross-shredded as soon as possible after the credit card billing transaction is completed.
* Only employees requiring access to payment card and electronic payment data in order to do their jobs are to be granted such access.

## Non-Compliance and Exceptions:

Cal Poly State University and its auxiliary organizations are contractually obligated to its acquirers to secure all credit card data captured, stored, processed, or transmitted. Failure to adequately secure credit card data resulting in a data breach may result in the following responses from the acquirers and/or card brands:

* Require Cal Poly to pay for a forensics team to investigate the breach
* Require Cal Poly to notify cardholders of the breach
* Impose implementation of additional expensive technical controls
* Impose costly quarterly security audits from third parties
* Assess fines that may reach hundreds of thousands of dollars or more
* Deny Cal Poly the ability to process payment cards

The Director of Student Financial Services may suspend/terminate credit card account privileges of any department or administrative unit not in compliance with this standard or that places the University at risk.

The Director of Student Financial Services will consider exceptions to this standard on a case-by-case basis in consultation with the Information Security Officer. In considering exceptions, the Director of Student Financial Services will examine compliance with applicable standards and the existence and reliability of compensating controls. Departments are responsible for obtaining written approval for any exceptions. Exceptions that put the University at significant risk must be approved by the President.

## Related Procedures and Resources:

* [Cal Poly Credit Card Acceptance web page](http://afd.calpoly.edu/fiscalservices/pci/index.asp)
* [Becoming a Credit Card Merchant at Cal Poly](http://afd.calpoly.edu/fiscalservices/pci/become_a_merchant.asp)
* [Cal Poly Credit Card Acceptance Channel Authorization Request Form](http://afd.calpoly.edu/fiscalservices/pci/cc-request-form.asp)
* [Payment Card Industry (PCI) web site](https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0)
* [PCI Data Security Standard: (PCI DSS)](https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0)
* [Cal Poly Information Retention and Disposition Schedules](http://afd.calpoly.edu/acs/recordretention/retentionschedules.asp)
* [PCI DSS Compliance Internal Assessment Questionnaire](file:///W%3A%5Cafd.calpoly.edu%5Cfiscalservices%5Cpci%5Cdocs%5CPCI%20DSS%20Compliance%20Internal%20Assessment%20Questionnaire%2006-02-14.pdf)
* [PCI Introductory Training](file:///W%3A%5Cafd.calpoly.edu%5Cfiscalservices%5Cpci%5Cdocs%5CPCI%20Powerpoint%2001-12-2012-%20Cal%20Poly%20Basic%20rev%2007-23-12b.pdf)