CAL POLY HUMBOLDT

EXECUTIVE MEMORANDUM

(P15-04) December 2015

SUBJECT: POLICY FOR COMPLIANCE WITH THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PURPOSE

The purpose of this policy is to ensure that credit card and e-commerce activities are consistent, efficient and secure to protect the interests of the University, its associated auxiliaries, and its customers. This policy applies to all types of credit card activity transacted in person, over the phone, mail or the Internet. This policy provides guidance to ensure that credit card acceptance and e-commerce processes comply with the Payment Card Industry Data Security Standard (PCI DSS) and are appropriately integrated with the University's financial and other systems.

POLICY

All card processing activities must comply with the Payment Card Industry Data Security Standard (PCI DSS) and the Cal Poly Humboldt PCI Standard.

Every department that would like to accept payment cards and/or electronic payments on behalf of the University or change an existing account must submit an APPLICATION FOR PAYMENT CARD ACCOUNT ACQUSITION OR CHANGE form to request approval http://www.humboldt.edu/studentfinancial/Downloads/pci_application.pdf. Each of these departments is required to appoint a management employee who will have authority and responsibility for payment card transaction processing within that department.

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 and services or make donations to the University. The payment card companies enforce compliance with this standard and, generally, non-compliance is discovered when an organization experiences a security breach that includes card member data.

Security breaches can result in serious consequences for the University and the associated auxiliaries including release of confidential information, damage to a reputation, the assessment of substantial fines, possible legal liability and the potential loss in the ability to accept payment cards and e-commerce payments.

SCOPE

This policy applies to all Cal Poly Humboldt and self-supporting operations, except the separate campus 501(c)3 auxiliary organizations (which include the Associated Students, Sponsored Programs Foundation and Cal Poly Foundation), 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.

With regard to auxiliary organizations, if they are contracting with the University for Accounting and Business Services, they must follow this policy. If not, the auxiliary needs to provide certification of PCI compliance to the University's Information Security Officer (ISO).

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.

RESPONSIBILITIES

Every department or administrative area accepting payment cards and/or electronic payments on behalf of the University for goods, services, or donations (merchant department) must designate a "Merchant Department Responsible Person" (MDRP), a management employee within that department who will have primary authority and responsibility for payment card and e-commerce transaction processing.

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 and in writing that they have read and understood this policy. These acknowledgements should be submitted, as requested, to the cashier manager.
- 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 the standard listed in Appendix 1 http://www.humboldt.edu/studentfinancial/Downloads/pci_appendix.pdf.
- In the event of a suspected or confirmed loss of cardholder data, the MDRP must immediately notify the Information Security Office and the c ashier manager. 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 (707) 826-5555.

POLICY MONITORING

The Department of Information Technology Services will coordinate the University's compliance with the PCI DSS technical requirements and verify the security controls of systems authorized to process credit cards.

The information security officer 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 information security officer shall conduct the University PCI DSS self-assessment and complete the University's attestation of compliance.

SUSPENSION

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

CAL POLY HUMBOLDT

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 approved by the Manager of Student Financial Services

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.

REFUNDS

The Cal Poly Humboldt Cashier's Office will process all credit card refunds on behalf of the University.

When a good or service is purchased using a payment card and a refund is necessary, the refund must be credited within the same billing period to the account that was originally charged. After that, the University will process the refund via check or ACH (electronic deposit to a bank account). Refunds in excess of the original sale amount or cash refunds are prohibited.

CHARGEBACKS (customer refunds)

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 Cal Poly Humboldt Cashier's Office and for providing appropriate supporting documentation.

TRAINING

Employees who are expected to be given access to cardholder data shall initially be required to complete security awareness training and then renew that awareness 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 (i.e., account number, expiration date, and cardholder name.)

Cashiering Services

University office that approves all third-party service providers and coordinates the policies and procedures for accepting payment cards at Cal Poly Humboldt.

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

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 the payment card and e-commerce 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.

CAL POLY HUMBOLDT

Appendix 1
Payment Card Industry Data Security Standards Program

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 this data with new requirements for software developers and manufacturers of applications and devices used in those transactions. Compliance with the PCI set of standards is mandatory for their respective stakeholders, and is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI Standards Include:
PCI Data Security Standard: The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts or processes payment cards, it must comply with the PCI DSS.

Penalties for Non Compliance:
Cal Poly Humboldt is contractually obligated to our Acquirers to secure all credit card data stored, processed or transmitted. Failure to adequately secure credit card data resulting in a data breach will invite the following responses from the acquirers and/or card brands:

- Force Humboldt to pay for a forensics team to investigate the breach
- Force Humboldt to notify card holders of the breach
- Impose implementation of additional expensive technical controls
- Impose costly quarterly security audits from third parties
- Assess fines up to about $650,000
- Deny Humboldt the ability to process payment cards

PCI Data Security Standard for Merchants & 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 common sense steps that mirror best security practices. The Goals of PCI DSS Requirements include:

Data Classification Standards:

The CSU Information Security Advisory Committee and information security staff from the Chancellor's Office have defined data classification standards as follows (see Appendix A):

- Level 1 Confidential Data: data governed by existing law or statute such as Social Security number, credit card number, or health information
- Level 2 Private Data: information that should be protected due to ethical or privacy concerns such as grades, disciplinary actions, or employment history

- Level 3 Public Data: information such as a person's title, email address, or other directory information

Policy:

Neither Level 1 Confidential data nor Level 2 Private data shall be stored on university–owned *personal computers* (desktop or laptop), other electronic storage *media* (e.g., cd, dvd, or flash drive) or other electronic *devices* (e.g., PDAs, smart phones) without the express written approval of the President or his designee. Approval shall only be granted in order to accomplish specific tasks identified as absolutely necessary to conducting the business of the University. The data shall be removed when the business reason no longer exists.

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

- All merchant sites must be authorized by the Cal Poly Humboldt Student Financial Services Manager (SFS Manager). See Application For Payment Card Account Acquisition or Change. Approval must be renewed annually.
- Service Level Agreements must be developed between Cal Poly Humboldt Cashier's Office and any department or entity processing credit cards.
- Departments seeking approval for accepting credit card payments must demonstrate that the physical location is secure and can provide limited access to unauthorized personnel.
- All merchant card services offered by the University must be delivered using software, systems, and procedures that are compliant with applicable standards.
- The Cashier's Office will authorize e-Payment services for use by Cal Poly Humboldt units.
- Units must coordinate the delivery of goods and services with the timing of charging e-Payments to customers as defined in the credit card operating regulations.
- The department selling the goods or services must comply with the CSU Cash Handling Policy for handling credit card. All forms used to collect credit card information must be approved by the SFS Manager.

Credit Card Merchant Numbers

- All credit card merchant sites must be established through the Cashier's Office. Departments are prohibited from obtaining merchant ID numbers directly from the credit card companies.
- Departments must use the campus provided third party provider for PCI compliance.

CAL POLY HUMBOLDT

Credit Card Transaction Channels

- Credit card information can be accepted through a Cal Poly Humboldt authorized web application, an approved wireless device, by telephone, mail, or in person only.
- Credit card information cannot be accepted via email and should never be e-mailed or sent by any other end-user messaging technology. 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 information cannot be accepted via fax. If a department receives a document with full credit card information, they will immediately notify the sender of the campus policy, process the credit card transaction and redact the document.
    - Departments are not permitted to transmit, process, or store credit card information on Cal Poly Humboldt computer systems, fax machines, the Internet, e-mail or any removable electronic storage (USB memory stick, hard drive, zip disk, etc.); not even if encrypted, without written permission from the SFS Manager.
    - The three or four digit validation code printed on the payment card, referred to as the Card Identification Number (CID), is never stored in any form; The CID number may also be referred to as the CVC2 and CVV2.
    - The full content 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;
    - If storage is authorized, 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;
    - If storage is authorized, credit card data must be encrypted at rest and in transit;
    - If storage is authorized, all media containing the full payment card or personal payment data is retained no longer than a maximum of six (6) months. After that time, the hard-copy materials are removed from the secure storage area and immediately cross-shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
    - If storage is authorized, hard-copy materials are never stored in storage containers awaiting disposal.
    - If storage is authorized, cardholder data must be encrypted across open, public networks;

CAL POLY HUMBOLDT

Credit Card Information Storage

- All hard-copy credit card information must be secured by authorized personnel at all times.
- The full credit card number should only be stored for the period of time needed to process the transaction.
- Credit card data should never be left unattended and may only be collected in designated areas at the University.
- Credit card data should be stored in a locked drawer, room or file cabinet with limited access if the transaction cannot be processed immediately.
- Any documents containing the full credit card number is classified as sensitive.
- Access to the storage area(s) must be limited to authorize personnel only.
- If a limited access, locked room or file cabinet, is not available, the records must be transported to the University Police Department and stored there in a secure location until the following business day when it can be retrieved by the Cashier's Office personnel.

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 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 the Cal Poly Humboldt Records Retention Schedule.

Fees, Reconciliations, Refunds & Disputes

- Departments are responsible for all credit card fees.
- There must be adequate separation of duty between any person authorized to issue a refund and the individual reconciling the account.
- Student Financial Services will be responsible to resolve all credit card disputes per the Cal Poly Humboldt return payment procedure. They will notify the department where the transaction was initiated.
- Refunds will be processed by the Cashier's Office and must be credited to the same credit card account from which the original purchase was made. After 90 days, the refund will be processed via check or ACH.
- The Accounting Department will reconcile credit card activity at least monthly.

Annual Self-Assessment & Network Scan

- Each department processing credit card payments will be required to assist the SFS Manager in completing the annual Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire. Once completed, the

questionnaire will be sent to the Information Security Officer for tracking and distribution.
- Departments will be required to resolve exceptions identified on the self-assessment questionnaire before the attestation can be completed. Departments should work with the Cal Poly Humboldt Information Security office to address any exceptions pertaining to technology or electronic storage.

Employees Handling Credit Card Information
- Only certified employees are authorized to handle or process credit card information for the University.
- Employees will be certified on a yearly basis by the SFS Manager. They will be required to complete the Cal Poly Humboldt PCI Compliance Security Training and the Data Security & Privacy Training.
- All employees, including volunteers who handle cardholder data must have a signed confidentiality agreement on file.
- When employees have access to payment card data, whether accepted via telephone, in-person, through the mail, or other non-electronic methods, the data must be secured before employee leave their workstation for any purpose.
- For special event phone drives where credit card payment data is written down prior to processing, the data must be physically transported via secure means to an authorized department for processing. It should not be sent via campus mail.
- The payment card data **may not** be retained by the employee or department.
- Only those with a "need-to-know" are granted access to payment card and electronic payment data.

Exceptions To These Responsibilities
The SFS Manager will consider exceptions to any of the above-stated responsibilities on a case-by-case basis in consultation with the Information Security Officer. In considering exceptions, the SFS Manager will examine compliance with applicable standards and the existence and reliability of compensating controls. Departments are responsible for obtaining written approval for any exceptions.

Cashier's Office Responsibilities:
- Establish and maintain a process for campus departments to accept credit cards.
- Approve applications from campus departments before credit cards can be accepted.
- Initiate and approve service level agreements with each department before credit cards can be accepted. Service level agreements will address the appropriate separation of duties within each department.
- Provide appropriate training to the campus on merchant card transactions.
- Apply for and secure all approved campus merchant ID numbers.

- Ensure credit card processing fees are properly charged back to the appropriate department in accord with Cal Poly Humboldt contracts.
- Initiate annual renewal of all service level agreements between the Cashier's Office and the departments.

Information Security Officer's Responsibilities

- Determining if the service provider is listed on the List of PCI-DSS Validated Service Providers (Visa websites).
- Obtain a Certification letter from a Qualified Security Assessor.
- Obtain a copy of the third-party vendors self-assessment; or
- Obtain the Service Auditors Report compiled under Statement on Auditing Standards (SAS) # 70.
- For all of the third party payment application software that stores, processes or transmits cardholder data as part of an authorization or settlement, verify, on an annual basis, that the third party application software is compliant with applicable payment card requirements.
- Ensure that each campus department that accepts credit cards completes the risk/security questionnaire/self-assessment required by applicable standards on an annual basis.
- Maintain a central file of all documentation indicating third-party vendor and third party payment application software compliance with applicable requirements.

Security Incidents and Loss of Card Holder Data

Department must notify the Information Security Officer and the SFS Manager 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 Cal Poly Humboldt State University Police at (707) 826-5555.

CAL POLY HUMBOLDT

I _____ certify that I have read the PCI Payment Card Industry Data Standards and fully understand the requirements for handling and processing credit card transaction. I understand that credit card information is Level 1 Confidential Data. I am expected to employ security practices as defined by EM P15-05, Policy for Compliance with the Payment Card Industry Data Security Standard and EM: P10-03, Cal Poly Humboldt Implementation of the CSU Data Classification Standards.

I understand that I am required to be re-certified every year.

I also understand that if I suspect a potential security breach or view any inappropriate activity surrounding credit card data storage or processing, I must notified the HSU Information Security Officer immediately or the Cal Poly Humboldt University Police.

_____ _____

Department Employee ID

_____ _____

Signature Date