HUMBOLDT STATE UNIVERSITY

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.

<u>PCI Standards Include</u>:
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.

<u>Penalties for Non Compliance</u>:
HSU 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 HSU to pay for a forensics team to investigate the breach
- Force HSU 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 HSU the ability to process payment cards

<u>PCI Data Security Standard for Merchants & Processors</u>:
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:

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 HSU 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 HSU 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 HSU 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.

Credit Card Transaction Channels

- Credit card information can be accepted through a HSU 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 HSU 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;

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 HSU 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 HSU 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 HSU 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 HSU 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.

Imprint Machines

Use of imprint machines must be approved by the SFS Manager.

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 HSU 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 Humboldt State University Police at (707) 826-5555.

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 P11-03, Policy for Compliance with the Payment Card Industry Data Security Standard and EM: P10-03, HSU 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 HSU University Police.

_____________________________ _____________________________

Department Employee ID

_____________________________ _______________

Signature Date