CAL POLY HUMBOLDT

Cash Handling Units Procedure Manual

1.0 Purpose

The purpose of this document is to establish procedures for cash collection points processing of collections based on the Integrated CSU Administrative Manual . (ICSUAM Section 6000). This manual outlines procedures for the establishment and maintenance of cash collection points, as approved by the Controller of Financial Services.

2.0 Objective

Cash collection procedures are used to ensure that controls are established to account for, collect and document in a timely manner the physical security of Cash and Checks over all University collections and to protect against and detect the unauthorized use of University funds.

Procedures have been designed to prevent fraud and theft of University revenues and assets. It is the responsibility of the university cash handler to adhere to these procedures and the designated separation of duties to reduce opportunity and access for the prevention of fraudulent activity.

3.0 Definitions

Cash Handling Units

- **Main Cashier/Bursar's Office** - The primary cash handling unit has the responsibility to collect, control, and maintain records for campus funds. Collections are deposited directly to an approved depository bank account.
- **Satellite Cashier** - Cashiering unit which generally performs cashiering activities as a primary function. Collections are deposited with Main Cashier.
- **Campus Cashier** - Department which performs minimal cashiering activities. For example, petty cash fund intended for minor departmental business expenses. Collections are deposited with Main Cashier.

4.0 Responsibilities

4.1 Controller of Financial Services

As delegated by Executive Memorandum 1000 the Chief Financial Officer of Cal Poly Humboldt or his/her designee will designate (1) authorized CSU personnel, Cashiers, who will function as the only employees authorized to handle incoming Cash and Cash Equivalents, and (2) Cash and Cash Equivalents collection locations that will function as the only authorized locations for incoming Cash and Checks. The Controller of Financial Services with assistance from the Cashier's Manager is responsible for monitoring and reviewing procedures regarding the processing of cash receipts.

4.2 Cash Handling Units

Each cash collection point is responsible for ensuring that all collections are made in accordance with established procedures. The collection point is responsible for ensuring that the cash processing function is segregated and appropriate internal controls are in place and operating effectively.

4.3 Cash Handling Unit Supervisor

Campuses are responsible for training designated employees in cash and cash equivalent handling policies and procedures. To ensure employee accountability, the supervisor of each Cash Handling Unit, must know who has authorization to cash and cash equivalent and to ensure each employee receives annual training. The supervisor will also be responsible for participating in the annual PCI Assessment and Certification.

5.0 Establish Cash Handling Units

5.1 Authorization

To accept payments on behalf of the university, you must be an approved cash handling unit. Complete Establishment of Cash Handling Unit Authorization Form with authorizing parties. The

Controller of Financial Services and Campus Risk Manager will approve all authorization forms. A site visit will be performed by the Cashier Manager and the Risk Manger prior to any approval to verify all safeguards are in place.

Departments will be require to re-certify their location each year. An annual site visit will be scheduled by the Associate Director of Student Financial Services. The cash handling coordinator for the department will be required to complete an in-person training and provide documentation of cash handling training for all staff.

Once approval has been obtained the Cashier's Manager will meet with the department to provide appropriate banking supplies, review staff training and discuss business processing for collection of cash and cash equivalents. All employees accepting cash will be required to complete yearly training on cash handling.

If credit card payments will be received at the location, all employees will be required to complete yearly PCI Training and certification.

6.0 Cash & Cash Equivalents Collection

Cash Equivalents -

- Cashier's Check - Any check which is drawn on a depository institution, signed by an officer or employee of such depository institution; and is a direct obligation of the depository institution.
- Certified Check - Any check certified by a depository institution that has set aside funds which are equal to the amount of the check; and will be used only to pay that check.
- Checks - Negotiable demand draft drawn on a depository institution that is a qualified member of the Federal Reserve System.
- Money Order - Financial instruments issued by a financial institution allowing the individual named on the order to receive a specified amount of cash on demand.
- Travelers Check - Preprinted, fixed-amount check.

If checks will be an acceptable means of payment:

a. All checks must be restrictively endorsed immediately upon receipt or by the end of day.
b. Payments must be payable to Humboldt State University or a reasonable variation.
c. Checks cannot be dated earlier than 180 days prior to the day of acceptance and no later than day of acceptance.
d. Checks cannot say "payable/paid in full" or be two-party.
e. No checks are to be cashed.to make an unconditional payment to someone else.
f. The written dollar amount should match the numeric dollar enter. The bank will post the check amount based on the written dollar amount.

Procedures and Internal Control Guidelines:

a. The cash handling unit should be staffed with two or more persons during times that payments will be accepted. Duel custody reduces the opportunity and access of any one cashier from university assets.

b. Only train cashier will be allowed to accept cash and cash equivalents at any cash collection point. Student employees must be supervised at all time by staff.

c. All employees with direct access to, or control over, cash, checks, other cash equivalents, credit cards and/or credit card account information are considered to hold Sensitive Positions and are subject to background checks in accordance with HR Coded Memo 2015-10 policy.

d. The person responsible for the cashiering input is the only person who can have access to the money collected and should safeguard the collections. Cashier must maintain a report of cash collections by tender (i.e. currency, check, other forms of payment).

e. The person who has access to collect/handle the money cannot authorize refunds and must obtain documented approval from supervisor or designee to void/cancel a transaction.

f. If payment is made in person, individual must receive pre-numbered sequential receipt. A collection not recorded on a cash register or the University Cashiering Software, "CASHNET" (Transact), or Audience View & Center Activities Fusion Software, must be recorded on a valid pre-numbered, multiple-part Cash Receipt. The receipts must be used sequentially. Receipt stock shall be kept secured, inventoried and regularly reviewed to prevent and detect alteration. Cash collection point should keep duplicate copy of the receipt.

g. Student or Employee ID numbers should be recorded on all payments when applicable.

h. Counterfeit currency retained by the bank are recorded as cash shortage. If counterfeit currency is detected in the Cashier's Office it is referred to the university police department.

i. All payments solicited to be received through the mail should be addressed to the Cal Poly Humboldt Cashier's Office. The cashier's office will process the payment timely, notify the department of the deposit, and provide any documentation needed. If payments are inadvertently received through the mail anywhere other than the cashier's office they must be logged, restrictively endorsed and follow procedures in "7.0 Depositing Payment" below.

j. Under no circumstances will payments be routed to other offices to obtain recording information. When the proper chartfield to which payment should be applied cannot be readily determined by the end of the business day, it will be deposited and recorded as "uncleared collections". Copies of the payment will be forwarded to departments to research correct recording instructions.

7.0 Depositing Payment

Procedures and Internal Control Guidelines:

a. Deposits must be verified against system generated or logged totals

b. Deposits must be sealed in a tamper-free bag or in a locked deposit bag

c. A cash receipt report must be prepared in advance to depositing funds at the cashier's office and should include: total amount deposited by type of payment, descriptions of overages/shortages and cashier responsible, name of person making deposit, chartfield to be applied, and any other pertinent information.

d. Satellite Cash Handling Units utilizing the Transact Cashiering System will be required to transfer deposits to the Main Cashier's Office on a daily basis.

e. Campus Cash Handling Units use alternative Point of Sale Devices, Fusion Cashiering System, tickets or hand receipts shall deposit to the Main Cashier's Office at least once a week or whenever excess cash exceeds $1,000.

f. Transportation of deposits must always be a high priority and should not conform to any regular schedule. Transporting deposits between Cash Handling Units will be accomplished in a secure manner to protect individuals, cash, and cash equivalents involved.

- Cash deposits under $1000 must be hand-carried by an authorized campus employee to the Main Cashier's Office.
- Cash deposits exceeding $1,000 must be transported by a campus police escort or armored car.
- Check should be restrictive endorsed and transported to the Main Cashier's Office by an authorized campus employee.

g. Upon delivery at the cashier's office a log will be signed by the cashier and the employees delivering the deposit.

h. The cashier's office will verify that the cash and equivalents agree to the deposit slip and system generated/logged total provided. The cashier's office will provide any documentation needed to the collection point.

i. If collections were not properly remitted to the cashier's office by the end of business day, it must be stored in a lockable receptacle with limited access.

- Deposits greater than $1000 must be stored in a safe.
- Deposits more than $2,500 must be stored in a safe with an appropriate alarm system.
- A log of individuals with access to the safe or vault must be maintained. The log should include the date the combination has been changed due to personnel changes.

8.0 Credit Card Payment

The cashier's manager has the authority to accept or reject requests for Campus Merchant Card Services from departments. The cashier's manager must approve all physical locations, websites, 3rd party processors or any channel accepting credit card payments. Credit card payments shall only be made at approved locations. All Departments will adhere to the University's PCI Compliance Policy including completing an Application for Payment Card Account Acquisition**.**

8.1 In-person transactions including point of sale terminals and wireless devices

Cashiering sites that accept authorized credit card transaction should use only Point of Sale terminals or equipment supplied to the location by the campus' Merchant Card processor.

Credit card receipts that are provided to the customer will be properly masked, showing only the last four digits of the credit card number. Detail log reports that are printed by each terminal prior to settlement will be brought to the Cashier's Office with the daily cashiering report. The Cashier's Office will process all campus credit card refunds by the department submitting a refund request.

8.2 Payment by Telephone

Telephone authorizations for payment shall be processed in a manner conforming to the National Automated Clearinghouse Association (NACHA) Operating Rules and compliant to relevant State and Federal rules and regulations.

Departments receiving credit card information over the phone must process the credit card transaction on their department terminal by the end of the business day then shred the credit card information. If the transaction cannot be immediately processed, it shall be temporally stored in a locked room or file cabinet with limited access.

8.3 Payment by Mail
The Cashier's Manager will approve all mail-in credit card solicitation forms departments would like to utilize prior to usage. All forms will be mailed directly to the cashier's office for processing. If departments receive credit card information through the mail inadvertently, they must:

1). Physically transport the mail to the cashier's office by a secure means or
2) Process the credit card transaction on their department terminal by the end of the business day then shred the credit card information. If the transaction cannot be immediately processed, it shall be temporally stored in a locked room or file cabinet with limited access.

8.4 Payment Online
All web transaction will be processed through one of the Universities' third party software, CASHNet (Transact), Fusion, Audience View, Passport Mobile Parking or CBORD GET. Departments must contact the cashier's manager to set-up a meeting to establish a Payment Card Industry (PCI) compliant interface and a CSU Third Party Provider. Departments are prohibited from obtaining merchant ID numbers directly from credit card companies.

8.5 Other important guidelines
Credit card information shall never be e-mailed.

Payment will not be accepted through fax.

Payment card data may not be retained by any employee or department.

Cash handling units are not permitted to transmit, process, or store credit card information on HSU computer systems. Documents with credit card information will never be left unattended on employee's desk or in plain view of others. Credit card information will temporarily be stored in a secure storage unit until it can be processed and shredded or transferred to the Cashier's Office.

9.0 Compliance Review

The controller of finance or designee will review campus compliance with the cash collection procedures on an annual basis.

As part of the University PCI Compliance Policy, each campus department or organization processing credit cards must:

- participate in an annual risk/security self-assessment questionnaire
- certify that all employees participate in an annual on-line PCI training
- certify that all employees review the HSU Cash Handling Procedure

Failure to comply with the established procedures will result in the Cash Collection Point's loss of cashiering privileges. If at any time staff is unable to maintain the required controls, he/she shall cease acceptance of cash and cash equivalents and contact Cashier's Manager for immediate assistance.

CAL POLY HUMBOLDT

Payment Card Industry Data Security Standards and Certification

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.

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 Associate Director of Student Financial Services.
    - 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 with the approval of the Associate Director of Student Financial Services
- 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.

Employees Handling Credit Card Information

- Only certified and trained employees are authorized to handle or process credit card information for the University.
- Employees will be certified on a yearly basis by the Associate Director of Student Financial Services. They will be required to complete the Cal Poly Humboldt PCI Compliance Security Training and the Data Security & Privacy Training.
- All employees 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. Credit card information should be locked in a cabinet, safe or cash drawer.
- 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.
- Employees will follow the Cal Poly Humboldt cash handling policy, any violation from the policy may result in the employee loosing cash handling privileges.

CAL POLY HUMBOLDT

Cash Handlers Certification of Training

Department/Organization _____

Trainer's Signature _____ Date _____

I certify that I understand the Cal Poly Humboldt Cash Handling and PCI Compliance Policy. I fully understand the requirements for cash handling, credit card processing and security of all university funds. I understand as an authorized employee of Cal Poly Humboldt, I am required to follow the policies for accepting, depositing, recording and safekeeping of cash, cash equivalents and credit card transaction. I understand that any variation of these policies without the preapproval from the Associate Director of Student Financial Services may result in a loss of cash handling privileges for myself and my Cash Handling Unit.

I have reviewed these policies and procedure with my department supervisor and/or the Associate Director Student Financial Services. I understand that I am required to be re-certified and trained every year.

I also understand that if I suspect potential fraudulent activity or if there is inappropriate activity surrounding the acceptance, storage or transportation of cash or cash equivalents on campus that I must notified my Supervisor, the Associate Director of Student Financial Services or the University Police Department.

Name	ID	Signature	Date

Revised May 2022