Cash Handling Procedures

Last Revised 09/08/2017

CSUSB Cash Handling Procedures

Submitted by: Marilyn Lymuel

Revision History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)	
09/08/2017	Sepi Harris	Changed title from Cash Handling Policy to Cash Handling Procedures; Minor revision to the safe requirements table; Credit Card Refunds	Title, IV, IX
08/17/2017	Marilyn Lymuel	Added link to CSU Retention Policy	VI
08/10/2017	Marilyn Lymuel	Updated Segregation of duties Section IV.	IV
07/24/17	Sepi Harris	Event Handling Section Added	XIX
07/24/17	Marilyn Lymuel	Updated policy regarding fingerprinting, separation of duties, mitigating controls	All
06/27/17	Sepi Harris	Petty Cash Section Added	XII
06/16/17	Marilyn Lymuel	Updated Policy to note types of Cashiering Offices; Updated Credit Card Refund Language	III
02/09/17	Sepi Harris	References to ICSUAM and SAM were updated	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
9/08/2017	Michael Zachary, Internal Audit	Approved
9/08/2017	Deletta Anderson, Dir. of Accounting	Approved
8/17/2017	Marilyn Lymuel, Manager of SFS	Approved
02/16/17	Marilyn Lymuel	Approved Updates
02/17/17	Deletta Anderson	Approved Updates
11/13/12	Deletta Anderson	Approved
11/13/12	Mike Zachary	Approved

CSUSB Cash Handling Procedures

Contents

I. Cash Policy of the University

Objective: The overall cash policy of the university, including campus auxiliaries, institutes controls and procedures to provide guidance for safeguarding cash and cash equivalents and to ensure that internal controls are established over all forms of payments, ensure that all payments are deposited promptly, ensure that cash receipts are protected from misappropriations, ensure that physical access to cash receipts is limited, provide a training tool for university and satellite cashiers, and provide uniform accounting rules.

Per **ICSUAM 3101.01**, it is the policy of the CSU that all money in the possession of, or controlled by, CSU will be deposited in the centralized bank(s) designated by the Executive Vice Chancellor/Chief Financial Officer (EVC/CFO) of the CSU.

Unless otherwise authorized by executive order, decisions regarding the administration and management of all CSU cash and investments are the responsibility of the EVC/CFO or his/her delegates.

II. Definition of Cash

The term "cash" as used in this document, refers to U.S. currency and coin, personal and business checks, traveler's checks, cashier's checks, money orders, credit cards, and ATM debit cards. Also included are items that are easily transferable or converted into currency like entertainment tickets and parking permits. E-Commerce debit, credit, and ACH transactions are also included in this definition.

III. Overview

All departments, including campus auxiliaries and other entities, collecting payments for goods or services must be delegated authority to do so by the Director of Accounting, prior to collecting payments. Departments responsible for collecting money have a fiduciary duty to adhere to all applicable state and University policies and procedures. Department heads, managers, cash handlers, and cashiers are responsible for those functions related to the receipts and deposit management. Individual accountability for cash shall be maintained throughout all cashiering operations. Initial training for cashiering and cash handling functions and an annual refresher training thereafter will be required for all employees handling cash.

To request authorization to collect payments, please complete a Request to Establish/ Maintain Cashiering Collection Point. Collection points at CSUSB are defined in three categories or three types of cash handlers:

1. **Main Cashier**: Student Financial Services, Palm Desert Campus Bursar Office, College of Extended Learning, and University Enterprises Corporation are designated as main cashiers.

2. **Department/Satellite Cash Handler**: Departments which frequently handle cash and cash equivalents, process payments and prepare deposits to a main cashiering point, and which

have been delegated authority from the Director of Accounting to collect payments.

3. **Occasional Cash Handler**: Handles cash infrequently. Inadvertently receives checks in the mail. These are not authorized cash handling points. Checks should be routed to a main or Departmental/Satellite cashiering point for deposit.

Per ICSUAM 3102.01, 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 2005-10 and/ or its successor policy.

The only exception to this policy is for temporary cash handling activities (e.g., parking attendants, ticket sellers) which may not warrant background checks. Instead, mitigating supervisory review controls should be employed in such instances.

The campus shall perform background checks and employment verification prior to employing cashiers or other cash handlers. Employment in a cash handling position is treated as provisional until the completion of the background check. Any felonies, misdemeanors, or judgments that were due to fraud related to cash, stocks, bonds or any other financial transaction should be addressed immediately.

Each department supervisor is responsible for arranging the appropriate background and employment verification when hiring employees into cash handling related positions.

The following requirements shall be satisfied as a condition of employment in a cash handling related position:

- Prospective employee's employment history verified.
- Other procedures as deemed necessary by the Internal Auditor given the circumstances (e.g. Credit Checks).

If an employee having cash handling responsibility is convicted of a felony or any crime related to cash, that conviction shall be reported to Campus Police, the employee's supervisor, Human Resources, Internal Auditor, and Accounting.

Each individual who receives or has custody of University cash and cash equivalents shall be held accountable for cash and cash equivalents under his or her control.

The campus CFO is ultimately responsible for ensuring that cash-handling training is delivered to all cash handling personnel.

IV. Internal Controls and Accountability – Cash Handling

Because cash is negotiable and easily transported, it is important for proper internal controls to be in place to protect this asset. Accountability requires the person to have the authority to carry out the task. An employee receives a delegation of authority to handle cash either through his/her job description that includes cash handling responsibilities or by approval from the Director of

Accounting. Any person who has delegated a task to someone remains accountable for ensuring the task is properly performed. Tasks can be delegated to someone only if that individual possesses the appropriate knowledge and technical skills.

Accordingly, it is the policy of the University that the following internal controls over cash receipts/handling be implemented throughout the University:

1. Cash receipts/handling operations must be subject to daily supervisory review.
2. Large sums of cash should be counted and handled out of sight of the general public. Deposits must be kept in a secure location throughout the day such as a safe or vault. All cash receipts must be completely and accurately recorded in the financial system of the University. To ensure this, Department Deposit Summary forms should be prepared for all cash receipts indicating the account(s) to which the funds are to be credited.
3. Checks must be restrictively endorsed immediately "For Deposit Only CSU San Bernardino."
4. Test hold-up and burglar alarms annually. Count change funds no less than weekly.
5. Use locked or tamper-free deposit bags for courier service. Never forward cash or cash equivalents via campus mail.
6. All change given in a transaction should be counted out to the customer. If an interruption occurs during the counting/change making, the process should be started again from the beginning. No checks are to be cashed, no IOU's allowed under any circumstances.
7. Have robbery prevention and safety procedures in place and periodically practiced. Immediately report to appropriate campus official's loss or suspected loss of cash.
8. Individual accountability must be maintained and documented for all cash handling procedures:
9. Each cashier shall be assigned a unique user ID, login, password, and cash fund not accessible by or shared with other individuals. The unit must provide a cash register drawer, a cash drawer insert or another secure cash receptacle to which only the cashier has access. An endorsement stamp or its mechanical equivalent will be provided. Where electronic deposit is available and completed by the close of business on the date of receipt, then restrictive endorsement is not required.
10. Cashiers must lock all cash in a drawer or other secure receptacle whenever leaving the immediate area.
11. Safe combinations, alarm codes and office keys shall be restricted to a minimum number of employees and should be changed periodically and in particular when there is a change in office personnel having said access.
12. A log shall be maintained of those entrusted with vault combinations and security gate keys. Indicate changes in personnel and include dates that the combinations are changed.
13. Safe access is to be restricted at all times. If access is necessary by any other person other than those designated, a designated employee MUST accompany that person (i.e. Armored Courier Service, safe repair, etc.).

Amount	Storage Requirement
$1.00-$1,000.00	Lockable receptacle
$1,001.00-$2,500.00	Safe
$2,501.00-$25,000.00	Steel-door safe, with a door thickness of not less than 1 inch and wall thickness of not less than ½ inch.
$25,001.00-$250,000.00	Class TL-15 composite safe or better
$250,001.00	Class TL-30 steel or better safe

V. Separation of Cash Handling Duties

A key element in a system of internal control is separation of duties. In accordance with **ICSUAM 3102.02**, duties are to be separated to the extent possible in every area that handles cash. Appropriate controls must be in place at all times. There is to be a system of checks and balances in which different individuals perform tasks for adequate control. Cash item handling, record keeping and reconciliation will be assigned to different people, even for agencies with automated accounting processes. A second person will verify reconciliation and deposit of cash items.

When complete segregation of duties is not possible, it is the appropriate departmental director or designee's responsibility to scrutinize all documents to ensure that the amount deposited includes everything that was collected. The following duties, when possible, should be assigned to different individuals to insure safeguarding of assets and the reliability of financial records.

- Cashiers shall not perform tasks incompatible with the collection and recording of receipts.
- The person collecting cash, issuing cash receipts, and preparing the departmental deposit should be someone other than the person performing the monthly review of the General Ledger or the person maintaining accounts receivable records.
- If campuses are unable to comply with this requirement for lack of resources, campuses must establish comparable, mitigating controls, approved by the campus auditor, that prevent and detect loss from fraud or negligence.
- Deposit counts should be verified by a second person.
- Collections for returned checks, credit card chargebacks and ACH returns should be processed by other than cashiering staff.
- The person approving write-offs should be different from the person maintaining the returned item inventory
- Accounts Receivable records shall be secured from alteration by other than designated personnel. Campuses shall maintain audit records of all changes to the Accounts Receivable records.
- Documentation of cash differences (overages and shortages) must be maintained for each cashier.
- Mailed remittances shall be verified, processed by a separate individual, and restrictively endorsed for deposit or electronically deposited by the close of business on the day of receipt.
- All cash transfers must be documented and the documentation of accountability maintained by category (i.e., currency, checks and other forms of payment).

Campuses shall make every effort to ensure that key tasks (e.g. receipt, reconciliation, entering journal entries) shall be performed by different personnel.

VI. Physical Protection of Cash and Cash Equivalents

The level of security necessary at each cash handling operation depends on the level of risk at that location. For example, the level of risk is generally higher at the central cash collection site of the University (the Student Financial Service's Office) than in an individual department that occasionally receives cash. To evaluate the level of risk at each location, the following factors should

be considered:

- Amount of money involved
- Geographic location
- Hours of operation
- Past loss experience
- Number of employees

In accordance with **ICSUAM 3102.04**, excess cash must be removed from the cash register drawer during the business day and transferred to a secure cash handling area/vault if it exceeds the amount that generally is required for daily operations.

At the close of business, all cash must be secured. Lockable receptacles or burglarproof/fire resistant safes to store cash and cash equivalents shall be utilized (refer to guidelines).

Where the guideline is less restrictive than what is required as a condition of liability coverage by CSU insurance carriers, the CSU shall conform to the requirements provided by the insurance carrier.

During the day if any cashier receives a large sum of cash or what appears to be a large sum of cash, the cashier will place the excess cash in the locking bag and place the bag in the safe.

If possible, the total receipts per bag will be verified in dual custody before the cashier leaves for the day. If not, the verification will take place the following day before the deposit is prepared.

Cash and cash equivalents must be locked in a secure receptacle or safe at all times except when signed out by a cashier for working cash. If the cashier needs to leave their work area for any reason, the cash drawer shall be secured.

Departments must implement physical security systems (i.e. alarms, panic buttons, motion detectors, security cameras, etc.) to ensure the safety of funds and personnel. If more than $2,500 in cash and cash equivalents is regularly on hand, a manual robbery alarm system or other appropriate measure must be installed for use during business hours to alert Campus police or local law enforcement in the event of a robbery or other irregularity. If more than $25,000 in cash and cash equivalents is stored overnight, an automated alarm system is required to alert Campus police or local law enforcement if the storage area is entered after business hours.

Safe combinations must be provided to the Student Financial Services Lead in a sealed envelope to be opened in the event of an emergency only. The Accounting Director's Office is responsible for keeping a record of the named individuals with knowledge of the combination to the safe.

A safe's combination must be changed whenever a person who knows the combination leaves the employ of a cash handling unit. Documentation must be maintained showing the date and the reason for the combination changes.

Each cashier must be provided with a separate lockable receptacle to which only that cashier has access. Duplicate keys must be sent to the Student Financial Services Office and be retrieved only

under dual control.

The physical setup of all cashiering stations must be reviewed by the Student Financial Services Office in concert Internal Audit personnel to ensure the safety of funds and personnel. Such reviews shall be in writing and retained per campus fiscal records retention policy.

Transporting deposits between cashiering sites or to the bank will be accomplished in a secure manner in order to protect the financial assets and individuals involved in transport. Transport shall be accomplished by at least two employees.

When deposits exceed $2,500, employees shall be escorted by campus police. When necessary, armored car service or police escort shall be used. When collections reach $250.00 in currency and coins, or $10,000 in all forms of payment, or have been held for 10 days, they must be deposited immediately to Student Financial Services Office. Use of security escort is encouraged when delivering deposits to Central Cashiering.

VII. Robbery Prevention and Safety

In accordance with the **State Administrative Manual (SAM) 8000**, state employees having custody of state funds will be instructed to surrender, without resistance, funds demanded if they are threatened with violence during the course of an attempted robbery. The University Police Department will be notified immediately. In addition, agencies are required to notify the Department of Finance, Office of State Audits and Evaluations.

ROBBERY PROCEDURES

- Be aware of your surroundings. Alert employees may make a robber nervous and think twice about the robbery.
- Keep visible cash low. Keep bait money in a strategic place so it can be included if you are robbed without arousing suspicion.
- Know where the silent alarms are and how to use them. Try to remain calm and not overreact.
- Comply with demands. Never take action that could endanger lives. Do nothing to alarm the robber.
- Keep the robbery note, if possible, but do not handle it, try to avoid rubbing out fingerprints.
- Discreetly observe robber and try to remember some basic characteristics such as sex, race, hair color, eye color, height, weight, unusual scars, tattoos, clothing, etc.
- Include bait with any money given to robber if it safe to do so.
- Do not jeopardize yourself or others by trying to activate the silent alarm prematurely. Press alarm when it is safe.
- Once the robbery is over, notify proper authorities.
- If possible, take note of the direction of the robber's escape. Do not chase the robber. Protect evidence. Do not touch the window area or anything the robber may have touched.
- Write down details of the robber and the robbery. Do not discuss them with other witnesses before discussing with law enforcement officials.

- Identify customers and staff who witnessed the robbery and might be able to give additional details to law enforcement officials.

VIII. Cash Overages & Shortages

Cash overages and shortages occur when:

- The incorrect change is given
- Mixing money between drawers
- Dishonesty
- The incorrect payment amount is posted to the system

In accordance with **SAM 8070**, state officers and employees who receive and disburse money will be held accountable for the money in their custody. They will be held personally responsible for any cash discrepancies. Cash Overages should be credited to an overage account at the time of receipt.

Overages:

SAM 8071 - If the person making the overpayment can be identified and the facts substantiated that an overpayment was made; refunds may be made and charged to the cash overage account. All other cash overages will be cleared as revenue or operating revenue at least once each quarter.

Shortages:

SAM 8072 - If all reasonable collection efforts do not result in payment, departments will adjust the accounting records by using the procedure applicable to the type of cash shortage that has occurred.

1. Shortages in excess of $100.00 must be reported to the Student Financial Services Lead immediately.
2. The supervisor will perform an audit of the cashier's drawer as soon as she is notified of the shortage. If the audit of the drawer results in a cash loss, the manager and director will be notified immediately.
3. Overages and shortages must be reported and explained on the cash transmittal form.
4. A review shall occur of all applicable resources which may include but is not limited to the following:
    a. CashNet vs. PeopleSoft posted amounts.
    b. Interview(s) with employee(s) in surrounding departments.
    c. Interview(s) with student(s) in or around department.
    d. Surveillance footage.
    e. Report filed with University Police Department.
5. If the overage/shortage is not reconciled, a Cash Overage/Shortage Form* must be completed including the following:
    a. Means and time/date of discovery
    b. Amount of overage/shortage and period covered. i.e. $250.00 – 06/04/10
    c. Name(s) of employee(s) who have access to funds/records
    d. Determine whether or not the employee(s) having custody of the funds used due diligence and followed recognized good practices in handling and safeguarding the funds.

e. Determine whether or not the overage/shortage was such as might reasonably be expected in the regular course of business and was not due to an employee's dishonesty, carelessness, or negligence.

6. Upon review of all facts if determined there was an employee infraction the following may occur:
   a. Documentation may be forwarded to the Human Resources Department to be included in the employee's permanent personnel file.
   b. Documentation may be included in the Supervisor's or Manager's employee personnel file.
   c. The infraction may be included on the employee's current evaluation form.
   d. The University Police Department may pursue legal activity.
   e. The University may terminate the employee.
7. Per CSU Executive Order 813, incidents of actual or suspected fraud involving State and/or non-state funds amounting to $1,000.00 or more will be reported to the VP for Administration and Finance no later than the first day following discovery of the irregularity.
8. The VP for Administration and Finance will notify the CSU Chancellor, Executive Vice Chancellor/CFO, University Auditor, and Chair of the Trustees' Committee on Audit within 24 hours after receiving the information.
9. Written reports will be forwarded to OSAE (Office of State Audits and Evaluations) and BSA (Bureau of State Audits) for incidents involving State funds.

IX. Acceptance of Cash and Cash Equivalents

Cash

- When cash is received, the transaction will be recorded in either an automated cashiering system (such as CashNet) or a pre-numbered cash log. The payer must be issued a receipt.
- Copies of manual cash receipts should be retained in numerical sequence, including any "voided" receipts.
- Employees handling cash receipts must balance cash collected to the cashiering system total or to the total of the manual cash log. Any difference in the total of the actual receipts and the total of the register or log must be reported as a shortage or overage.
- Cash must be balanced at the end of each employee's shift. Two employees may NOT work out of the same drawer.
- The duplicate copy of the manual receipt must accompany cash deposits when submitted to the Cashier's Office for processing.

In accordance with **ICSUAM policy 3102.03**, cash and cash equivalents should be deposited in a timely and cost-effective manner.

Departments may accept U.S. currency and coins only. Each Campus must comply with Federal and State Laws and Regulatory requirements governing transactions involving currency and coin.

Checks

All checks must be payable to: "California State University." Checks accepted by the University must contain all legally required elements including:

- Dating no earlier than 180 days prior to the day of acceptance (unless a shorter time period

is clearly marked on the face of the check)

- Checks may not be post-dated. Two party checks are not accepted. Personal checks cannot be cashed.
- Student ID numbers should be recorded on the face of all checks and money orders, including credit card transmittals when applicable. (To avoid privacy concerns SSNs should not be requested).
- Legible and consistent amounts, both numeric and written. Valid signature by the account holder.
- Checks bearing the legend "Payable/Paid in Full" are not to be accepted.

Checks drawn on foreign bank accounts are not acceptable. In the event that a foreign check is accepted in error at face value, it must be sent to and approved by the depository bank for collection within 30 days of receipt. The Internal Auditor may approve the use of alternate, fully documented, procedures for the handling and recording of checks drawn on foreign banks.

Checks, including mailed remittances, must be restrictively endorsed for deposit (endorsement stamp or its mechanical equivalent) or electronically deposited as soon as possible but not later than the close of business on the day of receipt.

Endorsement Stamps
The satellite cashier designees will be responsible for securing the University's bank endorsement stamp.

The Student Financial Services Office will be responsible for issuing bank endorsement stamps to satellite designees who have been approved to perform cashiering functions and to maintain appropriate records of issuance.

The Student Financial Services Office will also provide a copy of the applicable procedures. Satellite designees will be instructed to safeguard the endorsement stamp and be provided other training as necessary.

The Satellite designees will be responsible for reviewing the procedures and for securing the endorsement stamp in a locked drawer, safe, or vault.

Under no circumstances will checks be routed to other offices to obtain recording information. When the proper account(s) to which a check should be credited cannot be readily determined, it will be deposited and recorded as "un-cleared collections" and copies forwarded to departments to research correct recording instructions.

Reductions of recorded cash accountability, e.g., voids and reversals, must be supported by all copies of the document involved, explained, and approved in writing by the cashier's supervisor at the time of occurrence and retained per campus fiscal records retention policy.

An official CSU cash receipt should be recorded for each collection. A collection not recorded on cash register or point of sale equipment, including mailed payments, 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.

If the original receipt is lost, destroyed or otherwise unavailable as required by this policy, the campus may substitute a duplicate receipt that contains all of the elements of the original receipt and is clearly marked "duplicate", "copy" or some other designation that indicates that this item is not the original document.

All cash transfers must be documented and the documentation of accountability maintained by category (i.e., currency, checks and other forms of payment).

SAM 8022 – Documentation of Incoming Collections

- Department records will contain information regarding the type of collection (such as cash, check, or money order) received from each payer. This information will be recorded so that it can be readily audited from receipts, reports of collections, or the registers, and will show the amount of the check or money order presented.
- To maintain accountability of these assets, all incoming collections will be documented by the person opening the mail. These collections may be either payable or not payable to the state department.
- Cash or checks not payable to the department but are transferred between employees from the time of its receipt to its deposit will be documented by the department. This documentation will include the date received or check date/check number, payer name, amount, and a brief description of the receipt.

Some checks may have to be researched. If the purpose of the check cannot be resolved within 10 days, the check must be returned or deposited to the "SFS Uncleared" account.
If the check is not identified within 30 days after being placed in "SFS Uncleared" account, a check request should be prepared to return funds to the sender. The following procedures for checks/ACH should be adhered to:

- ✓ If a check is received that is not payable to CSUSB, the check should be logged, copied, and returned to sender.
- ✓ Electronic Based Cashier Point of Sale Equipment must meet the University security and operational standards.
- ✓ All cash registers and point of sale equipment must produce a cash receipt with a unique campus identifier assigned to each customer.
- ✓ The cash-recording equipment must be controlled by unique consecutive numbers generated automatically and recorded with each transaction, as well as imprinted on the customer receipt.
- ✓ The numbering mechanism providing consecutive transaction number control must be accessible only to the manufacturer's service representative or appropriate personnel who are independent of that cashiering station.

- ✓ Each cashier shall be assigned a unique user ID, login, password, and cash fund not accessible by or shared with other individuals.

Credit Card Payment Processing

In accordance with **ICSUAM 3102.05**, the Cash Handling Coordinator (Information Security Officer), as the designee of the campus CFO, has the authority to accept or reject requests for Campus Merchant Card Services from campus departments.

The Cash Handling Coordinator must approve of all physical locations, websites, 3rd party processors, or any channel accepting credit card payments. Credit card payments shall only be made at approved locations.

Cashiering sites accepting credit card payments should use only Point of Sale terminals or equipment supplied to the location by the campus' merchant card processor.

All 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. If any account number, cardholder name, service code, or expiration date is retained, it must be encrypted and protected according to the standards outlined in the Payment Card Industry (PCI) Data Security Standards.

Manual requests to process a customer's credit or debit card must contain all of the following elements:

a) Properly signed/executed authorization from the cardholder (unless processing over the telephone as provided for in NACHA guidance on TEL transactions),
b) Credit/debit card account number with expiration date,
c) The card holder's correct billing address,
d) Authorization codes, if the cardholder is not physically present.

Should a manual initiating document be created in certain circumstances (via imprint or manual transcription of card information), such documents must be secured, and retained and/or disposed of according to the records retentions schedules.

All University deployed gateways must operate in conformity with prevailing PCI Data Security Standards and must be compatible with the University's merchant card processor.

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.

The University will not accept payment by email or fax transmission.

The Student Financial Services Office does not accept credit card payments for tuition and fees at the window. Students must use the CashNet SmartPay system, which will accept Visa, MasterCard, Diner's Club, American Express, Discover Card, and electronic checks. There is a

service fee of 2.75% per transaction to the user for credit cards and no fee to users for electronic checks.

In order to ensure Payment Card Industry (PCI) compliance and to reduce liability, the University has adopted standardized procedures for accepting credit card payments that meet information security and audit standards required by CSU as outlined in the CSUSB ecommerce Security Standard. To review policies or request approval to accept credit cards go to https://wiki.csusb.edu/bin/view/Standards/InfoSec/ElectronicCommerceServices.

Web-Based Credit Card Payments

The University uses a PayPal account for campus programs, conferences, and events, to collect online payments. A PayPal account offers a flexible and cost effective alternative for campus departments to collect payments through the web.

The established PayPal account is managed centrally by the Accounting department, including processing withdrawals and refunds, as well as journalizing deposits into departments' trust funds.

The email address established for the PayPal account is onlinepayment@csusb.edu.This account has been set up so that all email notifications are forwarded to the individuals with access, and the mail group administration is performed by IRT.

In-Person Credit Card Payments

The campus uses Elavon as the preferred merchant account servicer for in-person payments. Elavon offers a secure PCI compliant payment solution with a variety of options for accepting in-person payments.

Credit Card Payment by Telephone

Credit card payments by telephone are not allowed unless approved by the Accounting Director.

Procedure for Requesting Approval for Credit Card Payments

The Student Financial Services Lead is the main point of contact for PayPal and Elavon inquiries. For approval to accept credit card payments, departments must complete a Request to Establish/ Maintain Cashiering Collection Point

Campus departments should be aware that there are fees associated with payments and refunds.

Internal controls

The email address associated with our PayPal account has been set up so that all email notifications are forwarded to the individuals with access, and the mail group administration is performed by IRT.

Access to the University's PayPal account is granted to the following individuals for processing, monitoring and reconciliation purposes:

- Director of Accounting
- Assistant Director of Accounting
- Student Financial Services Manager
- Student Financial Services Lead

A monthly reconciliation is conducted by the General Accounting department. General Accounting also records the journals to distribute payments to campus departments.

The Office of Information Security and the Internal Audit Office will conduct annual audits of department accepting credit card payments.

Credit Card Refunds
Student Financial Services processes credit card payments and related refunds for daily operations, using authorized lead, supervisory and management staff to review and approve such payments and refunds. Other locations that are authorized to process credit card payments are also authorized to process credit card refunds. All refunds must be approved by lead, supervisory, management, or other designated staff in the specific location that processed the payment. All locations that issue credit card refunds must document the refund transaction, including the approval, with forms or other evidence that adequately details the refund transaction.

In order to adhere to PCI Compliance requirements, locations that process credit card payments and refunds must first be reviewed and approved by the CSUSB Information Security group. Additionally, PCI Compliance requires that credit card payments will be refunded back to the original credit card if the refund request is made within 6 months; after 6 months, a refund will be sent by check.

Credit Card Chargebacks

Chargebacks are processed by the Student Financial Services Office upon approval by the department.

Reports
The Student Financial Services Lead provides reports to campus departments on a monthly basis or more frequently when needed for web-based Payments.

Information Security
The Information Security Officer is notified when new campus websites are created with a link to the university's PayPal account to ensure compliance with various security standards.

Credit Card Fees
The university's PayPal account has following fee schedule:

Purchase payments received (monthly)	Fee per transaction
$0.00 USD - $3,000.00 USD	2.9% + $0.30 USD
$3,000.01 USD - $10,000.00 USD	2.5% + $0.30 USD
$10,000.01 USD - $100,000.00 USD	2.2% + $0.30 USD
➢ **$100,000.00 USD**	1.9% + $0.30 USD

The $0.30 portion of the fee is non-refundable.

X. Returned Items

In accordance with **ICSUAM 3102.06**, all returned items must be processed and resolved in a controlled and timely manner.

Cash Equivalents and Checks:

- Physical security and accountability for returned cash equivalents must be maintained during the processing of the returned item.
- A non-cashiering unit is to provide processing of returned check items.
- Cash equivalents that are deemed to be uncollectible are to be returned by the depository bank to the designated non-cashiering unit.
- A returned cash equivalent must be redeemed by guaranteed funds. (For the purpose of this policy, guaranteed funds are any form of payment where a surety guarantees performance on the obligation. Examples include cashier's checks or money orders).
- The person maintaining the inventory of returned cash equivalents must not handle the cash received to redeem the returned items.

ACH (Automated Clearing House/E-Checks):

- ACH returned to the campus must be controlled during the processing of the returned item.
- A non-cashiering unit is to provide processing of returned ACH items.
- ACH transactions that are deemed to be uncollectible are to be returned by the depository bank to the designated non-cashiering unit.
- The person approving the request to write-off uncollectible ACH debits must not maintain the inventory of returned ACH debits.
- A returned ACH debit must be redeemed by guaranteed funds.
- Campuses shall establish controls to prevent and detect alterations to electronic ACH data.

Credit/Debit Card Charge-backs:

- Credit/Debit card charge-backs are to be returned by the Merchant Card processor to the designated non-cashiering unit.
- Cashiers must not be involved in the returned Credit/Debit Card chargeback, although they can be involved in defending the chargeback.
- A returned Credit/Debit Card chargeback must be redeemed by guaranteed funds.
- The personnel processing returned Credit/Debit Card chargebacks must not handle the cash received to redeem returned Credit/Debit Card chargebacks.
- The person who approves the request for write-off of uncollectible Credit/Debit Card chargebacks must not maintain the inventory of returned Credit/Debit Card chargebacks.

Counterfeit Currency:

- Counterfeit currency returned by the bank are recorded as a cash shortage and referred to campus university police department.

XI. Unidentified Receipts

In accordance with the University policy:

- Items must be pre-listed, and forwarded to appropriate entity (if identifiable), or returned to the payee no later than 30 days from receipt.
- Items made payable to a payee identifiable as a permutation or combination of the campus name or department may be deposited.

XII. Change Funds

In accordance with **ICSUAM 3102.10**, campuses shall establish procedures that maintain an adequate system of internal control to protect change funds from loss.

- All change funds must be established through the Accounting Director's Office.
- Cashiering and sub-cashiering locations shall establish change funds as required to support change-making activity.
- Cashiering and sub-cashiering locations are responsible for the security of their change funds.
- Accountability for change funds shall be assigned to an employee who is designated as the change fund custodian.
- Change funds should not be commingled with other funds.
- When change funds are no longer needed, or upon termination or departmental transfer of the custodian, change funds will be re-deposited at the cashiering office. Transfer of funds to a successor is not authorized. If a successor is to be furnished a change fund, a new request is required.
- The integrity of the change fund must be maintained at all times. Reconciliations of change fund balances shall be performed on a regular basis as determined by the campus CFO or delegate.
- An unannounced cash count and verification of change funds for which cashiers and cash handling employees are accountable shall be performed on a periodic basis as determined by campus procedure by someone other than the fund custodian. Verification of cash balances must be performed in the presence of the change funds custodian and must be documented.

XIII. Petty Cash

In accordance with **ICSUAM 3103.11**, petty cash funds may be utilized for the reimbursement of small dollar University business related expenses when payment by cash is the most cost efficient method of payment.

- The Director of Accounting Services may authorize establishment of petty cash funds at department offices or other approved locations. Requests/authorization for such funds must be documented in writing.
- A petty cash fund must be assigned to a specific individual as custodian. The custodian will be responsible for the amount advanced and should be trained on their responsibilities before accepting a petty cash fund. Evidence that the custodian has received the proper training should be documented.
- Petty cash funds must not be comingled with other funds.

- The petty cash fund will be closed out when a given petty cash fund is no longer needed, or upon termination or departmental transfer of the custodian. Transfer of funds to a successor is not authorized. If a successor is to be furnished a petty cash fund, a new request is required.
- With any one vendor or payee in a day, petty cash purchases may not exceed $50.00. Splitting a transaction into multiple reimbursements is not allowed.
- Expenses that cannot be paid from petty cash include, but are not limited to, the following: invoices from vendors, payments for services to employees or independent contractors, loans and advances.
- When not in use, the fund's currency and coin must be placed in a safe or locked receptacle kept in a properly secured area.
- An unannounced cash count and reconciliation of petty cash funds must be performed on a periodic basis by someone other than the fund custodian. The frequency of the periodic counts is based on the amount of funds at risk.

XIV. Deposits and Transfers to the Bank

In accordance with **ICSUAM 3102.11**, it is the policy of the CSU that bank deposits be made on a timely and secure basis and are supported with appropriate documentation. Accountability for and documentation of the custody of cash must be continuously maintained when preparing and transferring deposits to the bank.

The following operational controls have been implemented by the university:

- Collections made by cashiering locations depositing directly to the bank are deposited the same day as they are received, or at a minimum, on the following business day.
- Collections at other cashiering locations and departments are deposited at the designated main cashiering station at least weekly or whenever collections exceed $500.
- The depositing location is able to reconstruct transmitted deposits if necessary.
- All bank deposits are accompanied by appropriate documentation, such as a numbered deposit slip, system generated counts, or other bank requirements.
- Deposits are validated and prepared under dual custody so that all cash counts are confirmed by a second count performed by a different employee. The validation and preparation of cash deposits is conducted discretely in a safe and secure area.
- Before a daily bank deposit is finalized, cashiers reconcile receipts to deposits.
- Documentation signed by the preparer and recipient is maintained for each deposit to a main cashiering station from a cash-handling department or sub- cashiering station.
- If cash transfers after business hours are necessary, they will be secured in a locked receptacle to allow for passive acceptance of deposits.
- The main cashiering station records each deposit from a cash handling department or sub-cashiering station.

- A record of cash recorded and any overages or shortages is reported daily to the campus designated cash reconciliation unit. Supporting documentation is maintained (i.e., cash register audit tapes).
- If electronic-mechanical or electronic cash registers are not in use, a report of account of cash collections must be maintained.

Transmittal forms must be used for all deposits to the Student Financial Services Office. Forms must be prepared in advance and should include the following information whenever applicable:

- ✓ Total Amount Deposited
- ✓ Currency
- ✓ Coins
- ✓ Checks
- ✓ Brief description of reason for payments, Overages/Shortages, invoice numbers or other source documents.
- ✓ Name of individual or department making the payment being deposited.
- ✓ Account(s) to be credited and the amount credited to each account.
- ✓ Indication of whether the item(s) are taxable or nontaxable sales.

XV. Avoiding Deposit Errors

To prevent loss of satellite cashiering privileges, errors should be avoided. Satellite cashiers have the responsibility of ensuring that departmental deposits are balanced accurately. If designees are not cautious and errors regularly occur, satellite cashiering privileges will be revoked.

Common errors and problems that should be avoided include the following:

- Deposits are not in balance with the collection record or system generated totals.
- Rolled coins are not counted accurately.
- Check amounts are not written legibly.
- The currency totals do not balance with the total amount deposited. Departments can help to eliminate these errors by closely reviewing the information they record and by running duplicate tape totals on their deposits and corresponding paperwork.

XVI. Safeguarding Inventory

The following procedures should be followed to control and reduce the risk associated with inventory loss (i.e. parking permits, event tickets, pre-numbered receipts, retail stock, athletic inventory, library inventory):

- Verify the beginning inventory. This should be done in dual custody. Sign receiving paperwork to document the verification.
- Secure inventory in a safe or locked drawer.
- Safeguard inventory on hand by limiting and controlling access to inventory.
- Permits will be issued to cashiers by the Student Financial Services Lead; in the event of Lead's absence, a designated individual will issue the permits.
- Perform a physical inventory count on a predetermined frequency and submit counts

to Supervisor.

- Responsible personnel shall prepare a reconciliation of the inventory and cash collected. Variances, if any, are documented as part of the reconciliation. Variances over a specified limit are reported for investigation by the Department Supervisor.

XVII. Recording Deposits to the General Ledger

Per **ICSUAM 3102.08**, it is the policy of the CSU that all deposits be verified and recorded into the general ledger promptly and accurately.

Recordings to the General ledger and/or Receivable accounts must occur within an appropriate amount of time as determined by campus procedure but should be made within the same accounting period as the transaction.

Individuals with cash handling responsibilities cannot prepare or post journal entries.

All journal entries must be reviewed and approved by authorized employees in the Accounting Office. The preparer and reviewer/approver must be different persons.

All unidentified deposits will be posted to a specific "Uncleared Collections" account. The Accounting Office is responsible for researching and attributing items posted to the Uncleared Collections account. This account must be reconciled on a timetable consistent with Accounting's reconciliation policy.

XVIII. CashNet & Student Financials PeopleSoft Access Procedures

Per **ICSUAM 8060**, access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of need-to-know and least privilege.

Granting Access for CashNet – the request for access to CashNet (CashNet Security Access Form) is to be signed by the user's direct supervisor or manager and submitted to the CashNet Administrator.

Granting Access for PeopleSoft – the request for access to Student Financials PeopleSoft is to be submitted through a Computerized Information Access (CIA) Request Form and submitted to the Information Security Office. It is routed to the Student Financial Services Manager for authorization of access.

Removing Access for CashNet and PeopleSoft – a written request must be submitted to the CashNet Administrator for CashNet access and to the Information Security Office for PeopleSoft. It is the responsibility of department supervisors and managers to ensure that the request for removal of access is submitted in a timely manner.

Periodic Review of System Users – The Student Financial Services Manager is tasked with periodically reviewing CashNet and PeopleSoft users in order to identify users who no longer should have access, as well as to review the need for specific access rights. The level of access for valid users should also be

reviewed, along with specific access roles and rights. At a minimum, this review will be performed annually and whenever there are known staff changes or access changes that include new or updated CashNet access. An access review of PeopleSoft users who also have CashNet access will be performed as well. This review will focus on the need for PeopleSoft access, specific access roles, including whether they are excessive or unnecessary, and any PeopleSoft roles that might conflict with CashNet access.

XIX. Event Handling

Per **ICSUAM 13680.00**, it is the policy of the California State University (University) that accountability and responsibility for campus activities and programs be clearly established, and that related receipts are appropriately placed and controlled in University or Auxiliary accounts. This policy guides campuses as to the administration of such receipts and instructs as to their proper placement in accordance with legal and regulatory requirements.

Campus Events

Campuses normally host a wide range of activities in support of the operation of a campus and to complement the university experience not only for students, but also for faculty, staff, alumni and surrounding communities.
Examples include, but are not limited to:

- Music Concerts
- Conferences
- Intramural Sports
- Meetings
- Shared Interests Fieldtrips
- Youth Activities
- Athletic Camps
- Academic Ceremonies
- Debates
- Workshops

These activities may be provided by either the University or an auxiliary and are supported by ticket sales, registration fees, etc.

To request authorization to collect payments at campus events, please complete a Request to Establish/ Maintain Cashiering Collection Point.

XX. Failure to Comply and Mitigating Controls

Satellite cashiers who fail to comply with this document will be subject to internal audits and/or the immediate closure of their satellite cashiering operation.