POLICY STATEMENT

University departments that regularly collect cash, cash equivalents, and checks are responsible for ensuring that adequate control procedures have been put in place in order to safeguard such collections and that the funds are timely deposited with the University Cashier. Departments authorized to accept credit and debit card payments for the purchase of University goods or services or the acceptance of contributions must also ensure that adequate data security procedures have been implemented.

All departments responsible for the collection of cash, cash equivalents, and checks and/or the processing of credit and debit card transactions are subject to the standards set forth in this Policy.

REASON FOR POLICY

This Policy establishes the standards for the handling of cash, cash equivalents, and checks and the processing of credit and debit card payments received by the University. In addition, the Policy defines the roles and responsibilities related to the receipt, safeguarding, and deposit of cash.
WHO SHOULD READ THIS POLICY

Any employee who performs cash handling duties; the President, Vice Presidents, Vice Provosts, and Deans, as well as supervisors and Business Managers who supervise an employee with such responsibilities.

Policy Text

Depository Bank Account

All cash, cash equivalents, and checks collected by departments must be transferred to the University Cashier for deposit in the University’s depository bank account, in accordance with the procedures set forth in this Policy.

The authority to establish or make changes to the University’s banking and investment accounts is limited to the Vice President for Business and Finance, or his designee. No other person is authorized to open or make changes to a University banking or investment account.

Obtaining Approval to Accept Credit and Debit Card Payments

Departments must seek prior approval from the Associate Vice President for Accounting and Business Services to accept credit or debit card payments in connection with the sale of goods or services. Departments seeking such approval must submit a written request to the Office of Accounting and Business Services that responds to the questions contained in Appendix A.

Contributions and donations made with credit or debit cards are processed only by Development Services in the Office of Development.

Departments granted approval to accept credit and debit card payments will be provided with access to Commerce Manager or iModules, the University’s third-party e-commerce systems used for the processing of on-line credit and debit card transactions. Employees authorized to access Commerce Manager or iModules, however, must attend training prior to receiving access to the systems. See Appendix A.

Employee Background Checks

New employees must undergo a pre-employment background check prior to assuming any cash handling responsibilities. Departments must arrange with Human Resources to schedule a
background check, which will be conducted by the University's third-party service provider. See Background Check Policy.

**Petty Cash Funds**
Departments shall not establish or maintain a petty cash fund. Employees incurring out-of-pocket expenses for business-related purchases may be reimbursed by submitting an Expense Report and original receipts within 60 days of the transaction date through the Concur Reporting System. See Forms.

For a student who is not an employee, the preferred method of expense reimbursement is a Payment Request processed by a student's department through the Concur Reporting System. Reimbursements made through Concur may be paid by check or electronically directed into a student's bank account.

As an alternative, students may request reimbursements of up to $50 by submitting a completed Petty Cash Voucher and original receipts, approved by their applicable Business Manager, to the University Cashier. Such reimbursements are limited to three per fiscal year. When picking up cash, the student must sign the Voucher in the presence of the Cashier after providing his or her campus-wide identification. Cash pickups are subject to the Cashier's hours of operation.

Reimbursements processed through Concur are not subject to the dollar and frequency limits applicable to cash reimbursements.

---

**PROCEDURES**

- Separation of Duties
- Handling Cash
- Acceptance of Cash Equivalents and Checks
- Electronic Cash Registers and Point-of-Sale Equipment
- Processing Credit and Debit Card Transactions
- Sale of Admission or Event Tickets
- Preparing the DDR for Submission to the University Cashier
- Cash Receipts of More than $10,000
- Violations
RELATED INFORMATION

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>USF</td>
<td><strong>PCI Compliance</strong></td>
</tr>
<tr>
<td>USF</td>
<td><strong>Background Checks Policy</strong></td>
</tr>
<tr>
<td>USF</td>
<td><strong>Gift Acceptance Policy</strong></td>
</tr>
<tr>
<td>External</td>
<td><strong>Payment Card Industry (PCI) Security Standards Council, PCI Data Security Standard</strong></td>
</tr>
<tr>
<td>External</td>
<td><strong>PCI Security Standards Council, Payment Application Data Security Standards</strong></td>
</tr>
<tr>
<td>External</td>
<td><strong>FAQs Regarding Reporting Cash Payments of Over $10,000 (Form 8300)</strong></td>
</tr>
</tbody>
</table>

DEFINITIONS

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner System</td>
<td>The enterprise information system used to record the business activities of the University. The core system suite is made up of the Advancement, Finance, Financial Aid, Human Resources, and Student modules, and includes additional functionality in document management, job scheduling, reporting, and workflow.</td>
</tr>
<tr>
<td>Cash</td>
<td>Includes only U.S. currency and coins (except for purposes of Form 8300 reporting to the IRS).</td>
</tr>
<tr>
<td>Cash Equivalents</td>
<td>Includes assets that are readily convertible into cash such as money orders, traveler’s checks, cashier’s checks, and certified checks.</td>
</tr>
<tr>
<td>Check</td>
<td>A negotiable instrument instructing a financial institution to pay a specific amount from an account held in the drawer's name with that institution.</td>
</tr>
<tr>
<td>Commerce Manager</td>
<td>The University’s web-based system for processing on-line credit and debit card payments.</td>
</tr>
<tr>
<td>Credit Card</td>
<td>A card issued by a commercial bank or financial institution under the Visa or MasterCard brand or by an independent company (e.g., American Express, Discover, etc.) that permits the holder to pay for goods and services by drawing against a line of credit granted by the card issuer.</td>
</tr>
</tbody>
</table>
Debit Card
A card issued by a bank or financial institution under the Visa or MasterCard brand that permits the holder to pay for goods and services by drawing against available funds resident in the payer’s checking or savings account at the time of payment. Debit card transactions are processed either on-line (i.e., PIN debit) or off-line (i.e., signature debit).

Dual Custody
A task performed or an asset held in the control of two people.

FOAPAL
The acronym representing each element of the University’s Charts of Accounts, including Fund, Organization, Account, Program, Activity, and Location.

iModules
The University’s web-based system for event registration and processing of on-line credit and debit card payments.

ADDITIONAL CONTACTS

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Phone</th>
<th>Email/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting and Business Services</td>
<td>Frank Wasilewski</td>
<td>415.422.2402</td>
<td><a href="mailto:fmwasilewski@usfca.edu">fmwasilewski@usfca.edu</a></td>
</tr>
<tr>
<td>Cashier</td>
<td>Samantha Wilkinson</td>
<td>415.422.2579</td>
<td><a href="mailto:swilkinson@usfca.edu">swilkinson@usfca.edu</a></td>
</tr>
<tr>
<td>Disbursement Services</td>
<td>Dennis Miller</td>
<td>415.422.2102</td>
<td><a href="mailto:millerd@usfca.edu">millerd@usfca.edu</a></td>
</tr>
<tr>
<td>General Accounting</td>
<td>Jennifer Chan</td>
<td>415.422.2772</td>
<td><a href="mailto:chanjn@usfca.edu">chanjn@usfca.edu</a></td>
</tr>
<tr>
<td>ITS</td>
<td>Opinder Bawa</td>
<td>415.422.2787</td>
<td><a href="mailto:osbawa@usfca.edu">osbawa@usfca.edu</a></td>
</tr>
<tr>
<td>Payment Request</td>
<td>Emmy Moore</td>
<td>415.422.2706</td>
<td><a href="mailto:moore@usfca.edu">moore@usfca.edu</a></td>
</tr>
<tr>
<td>PCI DSS Training</td>
<td>Ivy Efendioglu</td>
<td>415.422.2731</td>
<td><a href="mailto:efendioglu@usfca.edu">efendioglu@usfca.edu</a></td>
</tr>
<tr>
<td>Tax Compliance</td>
<td>Dominic Daher</td>
<td>415.422.5134</td>
<td><a href="mailto:dldaher@usfca.edu">dldaher@usfca.edu</a></td>
</tr>
</tbody>
</table>

RETURN TO TOP
FORMS

<table>
<thead>
<tr>
<th>Form</th>
<th>Use</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department Deposit Record (DDR)</td>
<td>Used to transfer cash, checks, and credit card slips to the University Cashier for deposit</td>
<td>Accounting &amp; Business Services</td>
</tr>
<tr>
<td>Expense Report</td>
<td>Used in the Concur Reporting System to reimburse employees for business-related expenses paid with personal funds</td>
<td>Accounting &amp; Business Services</td>
</tr>
<tr>
<td>Petty Cash Voucher</td>
<td>Used to request reimbursement of incidental University expenses</td>
<td>Accounting &amp; Business Services</td>
</tr>
<tr>
<td>IRS Form 8300</td>
<td>Used to report cash payments of over $10,000 received by the University</td>
<td>Accounting &amp; Business Services</td>
</tr>
</tbody>
</table>

RESPONSIBILITIES

Department/Business Manager

- Prepares documentation to substantiate a request to pay an employee additional compensation for an activity authorized under this Policy.
- Reviews and approves requests to authorize the payment of additional pay for employees under his or her supervision.
- Secures the services of a temporary worker using the University’s preferred employment agency.

Payroll Services

- Processes additional pay through the payroll system and reports such payments and applicable withholding in accordance with IRS regulations.

Assistant Vice President, Human Resources

- Reviews departmental requests to pay out-of-classification pay or other additional pay as an exception to this Policy

President, Vice Presidents, Vice Provosts, and Deans

- Ensures that additional pay disbursed to his or her employees is in compliance with this Policy.
FREQUENTLY ASKED QUESTIONS

(None)

REVISION HISTORY

- 06/01/2015 - Updated to establish new limit for petty cash reimbursements made to students.
- 04/12/2013 - First publication of Policy.

APPENDICES

Appendix A  Requests to Accept Credit and Debit Card Payments

Appendix B  Physical Security of Cash Collections
PROCEDURES

- Separation of Duties
- Handling Cash
- Acceptance of Cash Equivalents and Checks
- Electronic Cash Registers and Point-of-Sale Equipment
- Processing Credit and Debit Card Transactions
- Sale of Admission or Event Tickets
- Preparing the DDR for Submission to the University Cashier
- Cash Receipts of More than $10,000
- Violations

SEPARATION OF DUTIES

Departments with cash handling responsibilities must ensure that no single individual is responsible for the collection, handling, depositing, and accounting of cash, cash equivalents, and checks received by the unit. Accordingly, the following departmental duties should be performed by separate individuals:

- Mail - Opens mail and distributes checks and cash equivalents to department cash handler.
- Cash Handler - Collects cash, cash equivalents, and checks; completes Departmental Deposit Record (DDR) for submission to the University Cashier.
- Ledger Reviewer - Reconciles departmental record of cash receipts to the general ledger on a monthly basis.

To the extent possible, a separate employee should be assigned to backup each of the individuals identified above when he or she is unavailable. In order to maintain adequate segregation of duties, the same employee should not be designated as the backup for more than one of these functions.

HANDLING CASH

Cash (i.e., currency and coins) is the most liquid form of payment and the most easily misappropriated. Cash handlers, therefore, must immediately establish a record of cash acceptance in accordance with the security standards set forth in this Policy. In addition, cash must be protected against loss upon receipt and at all points thereafter. To this end, departments with cash handling responsibilities must implement security procedures in accordance with the standards contained in Appendix B.

Departments shall not accept non-U.S. currency as payment.
ACCEPTANCE OF CASH EQUIVALENTS AND CHECKS

All cash equivalents and checks presented for payment should be made payable to the “University of San Francisco.” Departments should instruct their payers to use this name and not a variation of the University’s name (e.g., USF). Checks should never be made payable to an individual employed by the University. Invoices and other notices used to request payment should instruct payers that checks should be made out to the University of San Francisco. Checks should not be accepted if:

- The check date is 90 days or more prior to the date of receipt.
- The check has a future date, unless arrangements have been made with the payer to hold the check.
- The payment amount is illegible or the numerical dollar amount does not match the amount written on the check.
- The check is signed by someone other than the holder of the account.

In addition, departments are not allowed to cash personal checks.

Checks received that are drawn on a foreign bank account may require special handling procedures. The University Cashier should be contacted to determine the correct procedures.

Preparation of Receipts
Departments must prepare a receipt for each collection of cash, cash equivalents, and checks in accordance with the following procedures:

- Receipts must be pre-numbered and used sequentially.
- A copy of the receipt should be provided to each payer making an in-person payment.
- Receipt forms must be validated by the cash handling employee’s initials or signature, or by a validation stamp identifying the employee recording the transaction.
- All voided receipts must be retained (i.e., not given to the customer) and have signed approval by a supervisor.
- A receipt should be produced for a check payment received through the mail only when the payer has requested a receipt.

Receipts for donor contributions are prepared by the Development Office in accordance with the Internal Revenue Service’s (IRS) written acknowledgement procedures set forth in the Gift Acceptance Policy.
ELECTRONIC CASH REGISTERS AND POINT-OF-SALE EQUIPMENT

Electronic cash registers, micro terminals, and other point-of-sale (POS) equipment used by department cash handlers must meet the following security and operational standards:

- All cash registers and point-of-sale equipment must produce a University cash receipt for 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 University personnel who are independent of the cashiering function.
- Each cash handler must be assigned a unique identifier that is not shared by or accessible to other individuals.

The purchase of electronic cash registers, micro terminals, and other Point-of-Sale (POS) equipment used for departmental cash-handling operations must be approved in advance by the Vice President for Business and Finance and the Vice President for Information Technology Services (ITS), or their designees.

PROCESSING CREDIT AND DEBIT CARD TRANSACTIONS

All credit and debit card must be processed in accordance with the Payment Card Industry Data Security Standards (PCI DSS) adopted by the University. See PCI Compliance. In accordance with those standards, credit and debit card payments may be processed for both “cardholder present” and “cardholder not present” transactions, as follows:

Cardholder Present
Under these circumstances, the cardholder is physically on site to present his or her credit/debit card for “swiping” through the POS terminal. The transaction is completed when the authorization code is received and the cardholder has signed the card transaction receipt. The employee processing the transaction must verify the authenticity of the signature by comparing the signature on the receipt to the signature on the back of the credit/debit card. If the card has not been signed, the processor should ask to see the cardholder’s driver’s license.

Cardholder Not Present
When the cardholder is not physically on-site, the cardholder’s data (i.e., name, card number,
expiration date, billing address, etc.) would typically be collected by mail, telephone, or via a University website. This transaction is completed when the cash handler enters the cardholder’s information into the Commerce Manager or iModules POS terminal and obtains either an authorization code or rejection message from the system.

Mailed and telephone requests to charge a customer’s credit or debit card must be processed as follows:

- The authorization form must be correctly signed by the cardholder (mailed requests only).
- The credit or debit card account number and three-digit security code must be provided along with the card expiration date.
- The correct billing address for the credit and/or debit card must be provided.
- Prior to processing, all authorization forms must be stored in a safe or locked cabinet or drawer, accessible only by authorized persons, in order to protect cardholder information.
- When processing a debit card transaction, the PIN number should never be gathered or entered for the customer. PIN debit transactions are only allowed in a cardholder present environment where the customer enters the PIN directly into an approved keypad.
- After a transaction has been authorized by the system, only the last four digits of the account number and the authorization code may be retained. All other card information must be redacted or destroyed once a transaction has been authorized. Redacting stamps may be obtained from Accounting and Business Services.
- Departments should only store cardholder data for processing recurring payments. If cardholder data is stored electronically, it must be encrypted with access restricted to authorized persons with user ID and password protection. Hard copies of cardholder data must be stored in a safe or locked cabinet at all times.

For data security reasons, credit or debit card information should never be requested or transmitted via e-mail. Departments may accept credit or debit card payments via fax transmission only if the fax machine is housed in a secure location with restricted access.

All donor contributions made by credit or debit card are processed by the Development Office, which will send the donor a written acknowledgement confirming the receipt of his or her gift to the University. See Gift Acceptance Policy.

Note: Departments should not accept payments from another University department using the University Purchasing Card. The Purchasing Card is intended only for purchasing goods or services from third-party vendors.

**Point-of-Sale Equipment–Credit and Debit Card Processing**

All POS terminals and systems should be configured to prevent retention of cardholder data after a transaction has been authorized. If any cardholder data is retained, it must be encrypted
and protected in accordance with the standards outlined in the PCI DSS. See [PCI Compliance](#).

### SALE OF ADMISSION OR EVENT TICKETS

Procedures for the safeguarding and sale of admission or event tickets must meet the same standards and security requirements as those set forth in this Policy. Each ticket is considered both a product and a receipt. Tickets shall have the price of admission indicated thereon and shall be consecutively pre-numbered. When tickets are produced by electronic means, the numbering system must not be accessible to the ticket seller. All ticket sales must be balanced to recorded revenue on a daily basis by the department selling the tickets. The department must also develop adequate controls to safeguard the tickets and ensure that the number of tickets sold corresponds to the expected revenue from such sales.

A full accounting of all tickets sold or issued and payments received must be retained by the department for seven (7) years for audit purposes.

### PREPARING THE DDR FOR SUBMISSION TO THE UNIVERSITY CASHIER

Departments must use the following procedures when preparing the DDR to transfer collections of cash, cash equivalents, and checks to the University Cashier for deposit:

- Deposits must be transferred to the University Cashier on a weekly basis or sooner. If cash collections exceed $100, the funds should be transferred by the next business day, subject to the Cashier's hours of operation, or deposited in the drop box.
- The deposit must be validated and prepared under dual custody in a safe and secure area not visible outside of the cash-handling area.
- A DDR, signed by the preparer, must accompany each deposit delivered to the University Cashier.
- A report of any cash collections that are over or short must be sent to the University Cashier with the DDR, accompanied by supporting documentation (including cash register audit tapes, as applicable).
- The department should obtain a written receipt from the Cashier at the time the DDR is submitted for deposit.

When the proper FOAPAL to which a check should be credited cannot be readily determined, the DDR should be annotated by the department as follows: "Cash Received Undistributed." Under no circumstances should a check be routed to a department in another division for processing. Accounting and Business Services will follow up with the appropriate department to obtain recording information.
Appendix B contains additional information concerning the physical transfer of deposits from departments to the University Cashier. Departments, however, should not accept deposits from students for paying tuition, fees, room and board. Students should be directed to the One Stop Services Office, which has established several payment options to assist students in making such payments.

CASH RECEIPTS OF MORE THAN $10,000

The IRS requires tax-exempt organizations and other entities to report cash transactions of more than $10,000 received in the course of a trade or business on Form 8300. The reporting requirement applies only to actual cash transactions consisting of U.S. or foreign currency and coins received in one transaction or two or more related transactions. Funds received by cashier’s check, money order, bank drafts, or traveler’s checks are not subject to reporting, except for certain designated transactions generally not applicable to colleges and universities.

The University must file a Form 8300 with the IRS by the 15th day after the date of the cash transaction, or two or more related business transactions that occur within a 15-day period. For multiple related transactions, a Form 8300 must be filed within 15 days after an installment payment causes the total cash received within one year of the initial payment to exceed $10,000. Each person named on the Form 8300 must be provided with a copy of the form or a written statement by January 31, indicating that the information has been reported to the IRS. See Forms.

The Form 8300 is filed by the Director of Internal Audit and Tax Compliance when the University Cashier receives a reportable transaction(s).

VIOLATIONS

A violation of any portion of this Policy may result in disciplinary action, up to and including termination of employment and/or legal action. In addition, an employee may be personally liable for any financial loss incurred by the University as a result of the employee’s failure to comply with the requirements set forth in the Policy.
Requests to Accept Credit and Debit Card Payments
Appendix A

Departments requesting access to Commerce Manager or iModules in order to accept credit or debit card payments must obtain approval from Accounting and Business Services by preparing a request that addresses the following issues and questions

1. Please describe the nature of the payment activity and how the use of Commerce Manager or iModules will support this activity.

2. Is the volume of transactions sufficient to justify the processing costs and fees associated with credit or debit card acceptance?

3. Is it contemplated that a card other than Visa, MasterCard, or Discover would be accepted? If yes, please explain.

4. Does the department have a secure means of storing cardholder information provided by buyer at the point of sale or payment location? Please describe.

5. Does the department have a website? If yes, please provide the address.

6. Does the department’s processing environment comply with Payment Card Industry Data Security Standards (PCI DSS) requirements? See PCI Compliance.

7. Are procedures in place to protect personal or sensitive information from unauthorized disclosure or use, including compliance with state privacy standards and similar regulatory requirements?

Any contract for acquiring credit or debit card processing services must be reviewed by the Office of General Counsel, prior to being executed by Accounting and Business Services, for appropriate terms and conditions, including representations that service providers are PCI compliant and will assume financial liability for loss of any cardholder data while in the possession of the service provider.

Department staff approved to process credit and debit card transactions must undergo PCI DSS training before receiving access to Commerce Manager or iModules. See Additional Contacts.
Departments that regularly collect cash must establish the following procedures to ensure the physical security of such collections at all times, including when transfers of cash are made to the University Cashier:

- Cash must be locked in a fire-resistant safe at all times except when used for working cash.
- Excess cash must be removed from the cash register drawer during the business day and transferred to the safe. At the close of business, all cash must be transferred to the safe.
- Each department must use a fire resistant depository safe to store cash in accordance with the following cash limits:
  - Up to $25,000 - in a steel-door safe with a door thickness of not less than one half (½) inch.
  - More than $25,000 - in a class TL-15 composite safe or better.

Safes should be floor or wall-mounted to prevent their removal from the department’s premises. The purchase and installation of all safes must be approved by the Vice President for Business and Finance. In addition, the department must send a work order to Facilities Management to schedule the installation, if approved by the Vice President.

- If cash is regularly on hand, the department shall install a manual robbery alarm system for use during business hours to alert Public Safety if an emergency occurs.
- If more than $10,000 in cash is stored, the department must install security cameras and an automated alarm system to alert Public Safety if the storage area is entered after business hours.
- The safe’s combination must be given only to authorized personnel and their supervisors who must then commit the combination to memory. A record of the combination must be maintained in a sealed envelope away from the safe area. It should be sealed and opened only under dual custody to prevent unauthorized access.
- A safe that requires a combination and a key to gain access must have two different custodians. At least two employees shall be assigned the combination and two different employees shall be assigned a key. An extra key shall be sealed in an envelope, recorded, and maintained in the same manner as described above for a combination. Similar procedures must be maintained for a safe that requires two combinations to gain access.
- A safe must be opened in such a way that the combination is not viewed by other persons or security cameras.
- The safe must be locked between uses during business hours.
- A safe’s combination must be changed whenever a person who knows the combination leaves the employ of a cash-handling unit. In addition, the combination must be changed at least once a year. Documentation must be maintained showing the date and the reason for all combination changes.
- Duplicate keys must be safely stored away from the safe and be retrieved only under dual custody.
- Funds or property not related to the operation of the University must not be stored in the safe.

The Office of Internal Audit and Tax Compliance will periodically review the physical setup of department cashiering stations to ensure that appropriate security is provided.

**Collections Transferred to the University Cashier**

Department collections recorded on a DDR for deposit with the University Cashier will be transferred in a secure manner in order to protect the financial assets and individuals involved in transport.

- Deposits must be transferred by employees, in dual custody, transporting (walking or driving) the deposit to the Cashier. If the cash deposit is in excess of $1,000, employees should be escorted by Public Safety
- Campus mail shall not be used for transferring deposits of cash collections (or collections of cash equivalents and checks).

Any deviation from these procedures may adversely impact the University’s liability insurance coverage.

---

1 The dollar limits included in this Appendix apply only to collections of cash and not collections of cash equivalents and checks. Cash equivalents and checks, however, must be safeguarded in the same manner as cash to prevent their loss or misappropriation.