CASH HANDLING

Proc-3102.02
v. 1.4.2

PURPOSE

To provide procedures and guidance for accepting cash and cash equivalents, providing physical and electronic security of cash and cash equivalents and ensuring appropriate segregation of duties in accordance with *ICSUAM Policies 3101.02, 3102.02, 3102.03, 3102.04, 3102.05, and 3102.11.*

SCOPE

These procedures apply to any individual handling or processing University or Auxiliary Organization cash or cash equivalents.

DEFINITIONS

Cash

Coin and currency

Cash Equivalents

Checks, money orders, cashier's checks, and debit/credit card transactions containing cardholder data. (Credit cards processed at a satellite cashiering location, where a point of sale register or payment terminal produces a receipt which only contain the last 4 digits of the credit card number, is NOT considered a cash equivalent.)

Cardholder data

Includes the payment card number (credit or debit) plus any of the following:

- Cardholder name
- Expiration date
- Service Code

RESPONSIBILITIES

Chief Financial Officer

The Chief Financial Officer or designees' responsibilities are to:

- Authorize/Approve official campus cash collection points
- Appoint a PCI Data Authority
- Approve third-party vendors which collect cash and cash equivalents on behalf of the University

Cash Handling Coordinator

The Cash Handling Coordinator responsibilities are to:

- Ensure appropriate approvals have been obtained prior to establishing an official campus cash collection point
- Maintain a listing of all departments and MDRP's that perform cash handling duties
- Ensure cashiering stations are operating in accordance with CSU and University policy and procedures
- On an annual basis, distribute, review and administer the PCI Self-Assessment Questionnaire and PCI compliance program with departments who accept cardholder data
- On an annual basis, request local banks to search for unauthorized bank accounts that use the campus name, address and federal identification number

Payment Card Industry (PCI) Data Authority

The PCI Data Authority's responsibilities are to:

- Approve/Authorize department's ability to accept credit cards, which devices may be used to process, store, or transmit cardholder data, and the locations that can accept cardholder data.
- Specify the proper controls and procedures to protect cardholder data.
- Verify proper controls and procedures are in place to protect cardholder data.

Information Security Officer (ISO)

The ISO's responsibilities are to:

- Inform and advise the PCI Data Authority, CIO, and MDRP's about potential information security weaknesses that could lead to potential cardholder data breaches.
- Provide biennial risk assessments for PCI threats and risks to locations accepting cardholder data

Chief Information Officer (CIO)

The CIO's responsibilities are to:

- Provide PCI-DSS compliant telephone and networking infrastructure to MDRPs as needed
- Support MDRPs in setting up, configuring, and troubleshooting payment card technology in a PCI-DSS compliant manner

Merchant Department Responsible Person (MDRP)

Every department or administrative area accepting cash collections, payment cards and/or electronic payments on behalf of the University for goods, services, or donations (Merchant Department) must designate a Merchant Department Responsible Person (MDRP), an employee within that department who will have primary oversight responsibilities for cash collections, including payment card and eCommerce transaction processing. MDRP's shall be assigned by the applicable dean or senior director.

All MDRPs are responsible for:

- Annually executing the Request to Establish/Maintain Cashiering Collection Point (Form 3102.02-A) by June 1st.
- Ensuring that all employees, contractors, and agents with access to payment card data within the relative Merchant Department comply with the Payment Card Industry Data Security Standards in the manner(s) specified by the PCI Data Authority.
- In the event of a suspected or confirmed loss of cardholder data, the MDRP must immediately notify the Information Security Office. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notification shall be made to Sonoma State Police and Parking Services (707) 664-4444.
- Ensuring department cashiering procedures are in accordance with University and CSU policies and procedures

Risk Management

The Risk Management department's responsibilities are to:

- Review and approve the physical setup of all cashiering stations to ensure the safety of funds and personnel.

University Locksmith

The University Locksmith responsibilities are to:

- Provide the safe combination access or keys to applicable Safe Combination Coordinator
- Maintain a listing of all University safes and individuals with access to those safes
- Maintain a log of safe combination changes

Director of Internal Operations

The Director of Internal Operation responsibilities are to:

- Maintain a copy of the completed Safe Combination Coordinator Appointment form

PROCEDURES

1. **Cash Collection Points**
   A. The Cash Handling Coordinator should maintain a listing of all official campus cash collection points.
   B. Cash and cash equivalents shall only be received at these official cash collection points.
   C. To request approval to be setup as a cash collection point, or to modify or expand cash or debit/credit card activities, the department is required to submit a Request to Establish/Maintain Cashiering Collection Point (Form 3102.02-A). The department must not begin accepting cash or debit/credit card payments until the request has been approved. Cash collection points are approved for one fiscal year at a time, from July 1st to June 30th. All current cash collection points shall request renewal each fiscal year by submitting the form above along with the following documents to Financial Services by June 1st of each year:
      1. Cash Handling Annual Review Questionnaire (Attachment A to Form 3102.02-A)
      2. Cash Handling Segregation of Duties Matrix (Attachment B to Form 3102.02-A)
      3. The procedures for the satellite cashiering station. The procedures should include:
         a. Cash receipt collection process
         b. Deposit preparation and deposit process
         c. Review and reconciliation process
         d. Ensure position titles are used to describe who performs specific duties and to describe the individuals who are approving deposits, voids, etc.
         e. Procedures should be approved by MDRP by way of signature
   D. After signature from the department's dean or senior director, the form should be forwarded to the Cash Handling Coordinator for review and approval recommendation.
   E. The Cash Handling Coordinator shall ensure that the following requirements have been met before recommending approval of the collection point:
      1. Cashiers have had the required cash handling training (ICSUAM 3101.02)
      2. Cash, checks, and credit card information are physically protected (ICSUAM 3102.04)
      3. Appropriate segregation of duties are maintained (ICSUAM 3102.02)
   F. Upon approval recommendation from the Cash Handling Coordinator and the PCI Data Authority (if applicable), the form shall be sent to the Chief Financial Officer or designee for approval.

2. **Protection of Cardholder Data**
   A. All departments accepting payment cards (debit or credit) must comply with Payment Card Industry Data Security Standards (PCI DSS) in the manner(s) specified by the PCI Data Authority.
   B. Prior to accepting and capturing payment card data, all departments must obtain prior approval from Financial Services by completing the "Request to Establish/Maintain Cashiering Collection Point" form.
   C. Access to cardholder data must only be assigned only to roles that specifically require that privileged access.
   D. Cash collection points should use only Point of Sale terminals or equipment supplied to the location by the University's or Auxiliary's merchant card processor or acquirer to process or transmit cardholder data.

1. Payment terminals must be configured to prevent retention of the full magnetic stripe, card validation code, PIN, or PIN block cardholder data once a transaction has been authorized.
2. If any account number, cardholder name, service code, or the expiration date is retained, it must be encrypted and protected according to PCI DSS.

E. All paper and electronic media containing cardholder data (including receipts, reports, faxes, etc.) must be:
1. Kept physically secured, i.e. stored in locked cash register drawers or in other secured lockable receptacles or safes.
2. Strictly controlled when data is transferred from one individual or location to another and properly classified as sensitive data, i.e. cardholder data must be transported to the Main Cashier's Office in a sealed, tamper evident non-transparent money bag with at least two employees present when transporting.

F. Cardholder data may only be transported from the satellite cashiering location directly to the Main Cashier's Office. Approval from Financial Services management must be obtained prior to moving cardholder data to any other location or individuals.

G. All cardholder data must be cross-cut shredded, incinerated, or pulped when it is no longer needed for business or legal reasons within 90 days of the transaction, unless specific pre-approval has been granted by the PCI Data Authority.

H. Cashiers must be trained to be aware of suspicious behavior and to report tampering or substitution of devices that process credit cards. On a periodic basis, preferably on a daily basis as the cashier processes credit card transactions, the cashier must inspect credit card processing devices to look for tampering or substitution.

I. Departments not using only stand-alone payment terminals connected directly to the payment processor via a phone line must obtain explicit approval from Financial Services to use technologies in the card data environment, including desktop computers, laptops, ipods, remote-access programs, wireless networks, USB drives, PDAs, e-mail, and internet.

J. Credit card numbers may not be sent via end-user messaging technologies

K. The University may not accept payment by email or fax transmission.

L. Financial Services must maintain a current list of payment card acceptance devices which includes the make and model of device, location of device, serial number or other unique identification, and individuals with access to those devices.

3. Segregation of Duties

A. The Cash Handling Coordinator should maintain a listing of all departments and MDRP's who handle University cash or cash equivalents.

B. For each cash handling location, a segregation of duties matrix should be compared to the policy statements listed in policy 3102.02 to ensure proper segregation of duties.

C. Cash handling duties should be divided into three stages: receiving, recording, and reconciling. All three stages should be performed by different individuals.

D. If proper segregation of duties cannot be implemented for any cash handling function at any location, the Cash Handling Coordinator shall implement a mitigating control to ensure that University cash and cash equivalents are safe.

E. The Cash Handling Coordinator must document the appropriate mitigating controls and send to the CFO or designee for approval.

4. Cashiering Stations

A. Annually, the physical setup of all cashiering stations shall be reviewed and documented in writing by the Risk Management department to ensure the safety of funds and personnel.

B. All cash registers and point of sale equipment must produce a cash receipt controlled by consecutive numbers generated automatically and recorded with each transaction. This numbering mechanism must be accessible only to the manufacturer's service representative or appropriate personnel who are independent of that cashiering location.

C. Subsequent to the collection of funds, each cashier shall offer a copy of the receipt to the customer.

D. Each cashier should take reasonable precaution to detect counterfeit money prior to acceptance.

E. 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 or other secure cash receptacle to which only the cashier has access.

F. Prior to leaving the cash register or work area for any reason, the cashier shall verify the cash register is locked and secured.

G. As part of normal operations throughout the day, the cashier will accumulate cash receipts from sales. Excess cash of what is generally required for daily operations should be transferred from the register drawer to a University approved safe or lockable receptacle.

H. All cash registers and point of sale equipment must produce session closeout audit totals for verification to receipts collected. Reconciliation between the session closeout audit totals and the cash receipts collected must be reviewed and verified by someone other than the cashier responsible for the collections.

I. At the close of business, *all* cash must be secured and stored in accordance with CSU requirements as noted in procedure 11.0 below.

J. Documentation of cash differences (overages and shortages) must be maintained for each cashier and reviewed by the appropriate supervisor.

5. Payments Received Through Mail

A. If cash or checks are received regularly in the mail, the mail should be opened in dual custody. Payments received through the mail should be logged into the Cash Receipts Mail Log (Form 3102.02-B) and checks endorsed immediately upon receipt. Upon completion of the form the preparers should sign the log and forward the cash receipts and the log to the person preparing the deposit.

6. Official University Cash Receipt

A. An official University cash receipt shall be recorded for each collection using a cash register, point of sale equipment, or automated ticketing system, except in circumstances where it is not practical (i.e. event parking and payments received at department through the mail). In such circumstances departments must account for these collections in the following manner:

1. Pre-numbered tickets which are used sequentially, inventoried, and regularly reviewed to prevent and detect alteration, and where a ticket control log is reconciled to the deposit and reviewed by the appropriate supervisor.
2. Payments collected by mail should be logged onto the Cash Receipts Mail Log (Form 3102.02-C) and deposited to the Main Cashier's Office.

B. Departments who do not own a cash register or point of sale equipment may check out a cash register from the Main Cashier's Office for short term needs or events. Prior to check out of the cash register(s), the cashiers who will be operating the cash register must be trained by Financial Services for proper use of the equipment.

C. Generally, all payments should be collected using a cash register or point of sale equipment which automatically generates a receipt control summary. Departments wishing to collect payments via manual written cash receipts must obtain approval from Financial Services. This method will only be approved for departments where it is not practical to use an electronic cash register or point of sale system to account for receipts, and where the collection of payments are not a routine practice and where payments are small in dollar amount. If approved, the following requirements must be met (ICSUAM 3102.02 & 3102.03):
   1. Pre-numbered, multiple-part cash receipts must be used sequentially. Receipt stock shall be kept secured, inventoried and regularly reviewed to prevent and detect alteration.
   2. The storage and inventory of blank receipt stock must be handled by someone other than a cashier.

D. To document and maintain accountability, an official University cash receipt shall be provided whenever cash and cash equivalents are transferred between from one department to another, or whenever one person accountable for the deposit transfers the deposit to another person now assuming responsibility for the deposit. The cash receipt should break down the deposit by category (i.e., currency, checks and other forms of payment).

7. Voids and Refunds

A. Reductions of cash accountability, e.g., voids and refunds, must be supported by all copies of the document involved, explained, and approved in writing or electronically by the cashier's supervisor at the time of the occurrence and submitted with the deposit supporting documentation.

8. Requirements of Checks Received

A. All checks must be payable to Sonoma State University, Sonoma State University Academic Foundation, Inc., Sonoma State Enterprises, Inc., Associated Students, Incorporated of Sonoma State University, or reasonable variations thereof.

B. Checks accepted by the University must contain all legally required elements including:
   1. 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) and no later than the day of acceptance.
   2. Legible and consistent amounts, both the numeric and written.
   3. Valid signature by the account holder.

C. The following procedures should be followed for checks that do not contain all the legally required elements noted in procedure 8.B. above:
   1. Checks received in person from the payor should be reviewed at the time of receipt for the required elements noted in procedure 8.B. If any of the required elements are not met, the cashier must return the check to the payor for correction.
   2. Checks received in the mail from the payor should be reviewed at the time of receipt for the required elements noted in procedure 8.B. If any of the required elements are not met, the cashier should make every effort to contact the payor to request a new check be issued. The

cashier should mail the invalid check back to the payor, if possible, otherwise shred the check.

D. All checks must be verified, processed, and restrictively endorsed (endorsement stamp or its mechanical equivalent) by the close of business on the day of receipt and kept secured in a locking drawer or safe.

E. Checks should not 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 should be deposited and recorded as "uncleared collections" and copies forwarded to departments to research correct recording instructions.

9. Deposits

A. Deposits should be prepared by an individual who does not have access to recording transactions (i.e., should not have access to post journal entries), authorizing adjustments to the accounts receivable ledger or to the general ledger, or the person following up on collectibles.

B. Deposit counts shall be verified by a second person. For departmental deposits, all deposits will be verified by the main cashier's office.

C. Deposits should be reviewed and verified/reconciled to the general ledger by an individual who is not part of the deposit process and does not have access to cash. This provides an independent verification that the amount recorded on the supporting deposit documents was the amount that was actually deposited. When this reconciliation is not practical or feasible due to personnel restraints, other compensating controls should be established through consultation with the Cash Handling Coordinator.

D. The Main Cashier's Office or any other cash location that deposits directly to the bank must deposit collections by the following business day. Satellite cashiering location collections must be deposited to the Main Cashier's Office within five business days of receipt. All deposits should be supported by a completed Deposit Transmittal Sheet, CASHNet Summary Report, or Audience View Report.

E. Transporting of deposits should be in a sealed, tamper evident non transparent money bag with the tear off slip retained by the originating office.

F. Transporting of deposits between cashiering stations or to the bank should be accomplished in a secure manner. In order to protect the financial assets and individuals involved, the transport of all deposits of cash and cash equivalents shall be accomplished jointly by at least two employees. When transporting deposits of cash exceeding $1,000 or cash and cash equivalents that accumulatively exceed $5,000, employees must be escorted by campus police.

10. Single Cash Transaction > $10,000

A. Any single *cash* transaction or two or more related cash transactions for more than $10,000 that is received by a cashiering location must be communicated to the Cash Handling Coordinator. This transaction must be reported to the IRS using IRS form 8300, Report of Cash Payments over $10,000 Received in Trade or Business on or before the 15th day after the date of the cash transaction, or two or more related business transactions that occur within a 15-day period.

11. Security of Cash Funds

A. The following are the requirements for storage of cash:

1. Up to $1,000 in a lockable receptacle

2. $1,001 to $2,500 in a safe
3. From $2,501 to $25,000 in a steel-door safe, with a door thickness of not less than 1 inch and wall thickness of not less than ½ inch.
4. From $25,001 to $250,000 in a class TL-15 composite safe or better.
5. Over $250,000 in a class TL-30 steel safe or better.

B. Physical security systems are required in areas where large amounts of cash are collected
1. 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 law enforcement.
2. If more than $25,000 in cash and cash equivalents is stored overnight, an automated alarm system is required to alert law enforcement if the storage area is entered after business hours.

12. Safes/Lockable Receptacles

A. All purchases of safes are handled by the University Locksmith. An individual must submit a work request to Facilities with the appropriate dean or senior director's approval. Upon receipt of a work request for the departmental purchase of a safe, the University Locksmith will contact the requestor to determine the type of safe that should be ordered.

B. The order, delivery from vendor, and delivery and installation of safe to the department are the responsibility of the University Locksmith.

C. Safes should be bolted to the ground or wall and such activity must be coordinated through the University Locksmith.

D. The relocation or removal of existing safes must only be performed by the University Locksmith.

E. Lockable receptacles that store cash, checks or credit card information should always remain locked when not in use and should be stored in a locked desk, cabinet, or office when not in use for operations.

F. Each safe must be assigned a Safe Combination Coordinator by the appropriate dean or senior director using the Safe Combination Coordinator Appointment (Form 3102.02-C). A copy of the completed form must be forwarded to the University Locksmith.

G. Each Safe Combination Coordinator must maintain a written record of authorized persons who know the combination of the safe and the date the combination was last changed.

H. Combination access changes may be requested by the Safe Combination Coordinator by submitting a work request to Facilities. When a combination is issued or changed by the Locksmith, the Safe Combination Coordinator and Locksmith shall sign the Safe Combination Access Listing (Form 3102.02-D). The Locksmith must provide a copy of the form to the Director of Internal Operations to provide notice of a safe access change.

I. The Safe Combination Coordinator must list the names of the individuals who have been provided the safe combination on the Safe Combination Access Listing (Form 3102.02-D) and retain for recordkeeping.

J. The combination should be known to as few persons as possible consistent with operating requirements and the value of the cash or documents.

K. The combination must be changed when the code becomes known to an excessive number of employees, or if any employee having knowledge of the combination leaves the employ of the agency, or no longer requires the combination in the performance of his or her duties.

L. Certain departmental safes have been identified by the CFO, where in the case of an emergency the CFO may need access to the safe. The CFO or designee shall communicate to the University Locksmith which safes the CFO may need access. The University Locksmith shall give the Assistant to the Vice President the new combination code for safe keeping whenever the code is changed. The code information is contained in a sealed envelope with the safe location, name of the safe combination manager, and date of the latest code change noted on the envelope.

13. Door Combinations

A. Certain areas are kept secure through the use of electronic keys and/or keypad combinations. Secured areas that require the use of an electronic key and/or keypad combinations shall only obtain access to the secure area by following the official University "Key Control" policy and "Key Issuance Procedures".

14. Securing Against Unauthorized Bank Accounts

A. On an annual basis, the Cash Handling Coordinator shall request local banks via a written letter to search for unauthorized bank accounts that use the University or auxiliary organizations' name, address and/or federal identification number.

B. The Cash Handling Coordinator shall forward the local list of banks along with the written responses from the banks to the University Controller for review by way of signature.

C. Any unauthorized accounts must be investigated and reported to the University Controller so applicable steps can be taken to close the unauthorized bank account.

POLICY/PROCEDURE CONTACT INFORMATION

Unit	Contact Name	Title	Phone	Email
Financial Services	Brian Orr	Sr. Director – Student Financial Services	x4462	Brian.orr @sonoma.edu

APPROVAL AND REVISION HISTORY

Policy Owner Approval	Title	Policy Committee Approval Date	Effective Date	Version	Description of changes
Letitia Coate	AVP A&F	4/20/16	4/20/12	v 1.0	Initial Release
Brian Orr	Sr. Director Tax, Policy & Compliance	5/1/14	5/1/14	v 1.1	Removed Information Security Officer from approval process. Other minor changes.
Brian Orr	Sr. Director Tax, Policy & Compliance	6/12/14	6/12/14	v1.2	Added responsibilities for PCI security. Added section 2, "Protection of Cardholder Data". Added definition of "Cardholder data".
Brian Orr	Sr. Director Tax, Policy & Compliance	6/1/15	6/1/15	v1.3	Added additional PCI requirements to section 2 "Protection of Cardholder Data" per PCI standards. Updated hyperlinks.
Brian Orr	Sr. Director Tax, Policy & Compliance	2/3/16	2/3/16	v1.4	Added to CFO responsibilities: "Approve third-party vendors which collect cash and cash equivalents on behalf of the University"
David Crozier	Sr. Director for University Financial Services	8/29/16	8/29/16	v1.4.1	1. Remove references to Student Union. 2. Update definition of cash equivalents to exclude credit cards receipts already processed with the card processor. 3. Add language that requires deposits are required whenever cash and cash equivalents exceed $500. 4. Add language that requires campus police escort for deposits of cash equivalents over $2,500.
David Crozier	AVP – Financial Services	9/20/2017	9/20/2017	v1.4.2	1. Added requirement 6.D. to require cash receipt be issued when transferring deposits between departments/individuals 2. Removed $500 limit for when deposits must be submitted to Main Cashier's Office. Changed timeline for deposit requirement from 2 days to 5 days. See section 9.D. 3. Changed section 9.C. amounts for when police escort is required.