




<u>Subject:</u> Cash Handling Procedures	<u>Department Name:</u> Financial Services	<u>Effective Date:</u> 10/01/2016 <u>Issue Date:</u> 10/01/2016
	Revised Procedure	<u>Approval:</u>  Darrell Haydon, VP B&F (CFO)

## **CASH HANDLING PROCEDURE**

### **A. PURPOSE**

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

### **B. SCOPE**

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

### **C. DEFINITIONS**

**Cash** - Coin and currency

**Cash Equivalents** - Checks, money orders, cashier's checks, and debit/credit card transactions

**Cardholder data** - Includes the payment card number (credit or debit) plus any of the following:

- Cardholder name
- Expiration date
- Service Code

### **D. RESPONSIBILITIES**

#### **Chief Financial Officer (CFO)**

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 (Director of Cashiering & Cash Management)**

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 Department Responsible Persons (DPR) that perform cash handling duties
- Ensure cashiering stations are operating in accordance with CSU and University policy and procedures
- On an annual basis, request local banks to search for unauthorized bank accounts that use the campus name, address and federal identification number
- Maintain a copy of the completed Safe Combination Coordinator Appointment form

#### **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.
- On an annual basis, distribute, review and administer the PCI Self-Assessment Questionnaire and PCI compliance program with departments who accept cardholder data

#### **Information Security Officer (ISO)**

- The ISO's responsibilities are to:
- Inform and advise the PCI Data Authority, CIO, and DRPs 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 DRPs as needed
- Support DRPs in setting up, configuring, and troubleshooting payment card technology in a PCI-DSS compliant manner

#### **Department Responsible Person (DRP)**

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 Department Responsible Person (DRP), an employee within that department who will have primary authority and responsibility for cash collections, including payment card and eCommerce transaction processing. DRPs shall be assigned by the applicable dean or senior director.

All DRPs 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 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 DRP must immediately notify OIT- Office of Information Technology. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notification shall be made to Stanislaus State Police Department (209) 667-3114.
- Ensuring department cashing 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 cashing 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

## **E. PROCEDURES**

### **Cash Collection Points**

1. The Cash Handling Coordinator should maintain a listing of all official campus cash collection points.
2. Cash and cash equivalents shall only be received at these official cash collection points.
3. 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:
  - a. Cash Handling Annual Review Questionnaire (Attachment A to Form 3102.02-A)
  - b. Cash Handling Segregation of Duties Matrix (Attachment B to Form 3102.02-A)
  - c. The procedures for the satellite cashiering station. The procedures should include:
    - i. Cash receipt collection process
    - ii. Deposit preparation and deposit process
    - iii. Review and reconciliation process
    - iv. Ensure position titles are used to describe who performs specific duties and to describe the individuals who are approving deposits, voids, etc.
    - v. Procedures should be approved by DRP by way of signature





4. 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.
5. The Cash Handling Coordinator shall ensure that the following requirements have been met before recommending approval of the collection point:
  - a. Cashiers have had the required cash handling training (ICSUAM 3101.02)
  - b. Cash, checks, and credit card information are physically protected (ICSUAM 3102.04)
  - c. Appropriate segregation of duties are maintained (ICSUAM 3102.02)
6. 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.

#### **Protection of Cardholder Data**

1. 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.
2. 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.
3. Access to cardholder data must only be assigned only to roles that specifically require that privileged access.
4. 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.
  - a. 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.
  - b. If any account number, cardholder name, service code, or the expiration date is retained, it must be encrypted and protected according to PCI DSS.
5. All paper and electronic media containing cardholder data (including receipts, reports, faxes, etc.) must be:
  - a. Kept physically secured, i.e. stored in locked cash register drawers or in other secured lockable receptacles or safes.
  - b. 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.
6. 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.
7. 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.
8. 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.



9. 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, iPad, remote-access programs, wireless networks, USB drives, PDAs, e-mail, and internet.
10. Credit card numbers may not be sent via end-user messaging technologies
11. The University may not accept payment by email or fax transmission.
12. 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.

#### **Segregation of Duties**

1. The Cash Handling Coordinator should maintain a listing of all departments and DRP's who handle University cash or cash equivalents.
2. 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.
3. Cash handling duties should be divided into three stages: receiving, recording, and reconciling. All three stages should be performed by different individuals.
4. 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.
5. The Cash Handling Coordinator must document the appropriate mitigating controls and send to the CFO or designee for approval.

#### **Cashiering Stations**

1. 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.
2. 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.
3. Subsequent to the collection of funds, each cashier shall offer a copy of the receipt to the customer.
4. Each cashier should take reasonable precaution to detect counterfeit money prior to acceptance.
5. 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.
6. Prior to leaving the cash register or work area for any reason, the cashier shall verify the cash register is locked and secured.
7. 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.
8. 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.

9. At the close of business, all cash must be secured and stored in accordance with CSU requirements as noted in procedure for **Security of Cash Funds** section of this document.
10. Documentation of cash differences (overages and shortages) must be maintained for each cashier and reviewed by the appropriate supervisor.

#### **Payments Received Through Mail**

1. 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.

#### **Official University Cash Receipt**

1. 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:
  - a. 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.
  - b. Payments collected by mail should be logged onto the Cash Receipts Mail Log (Form 3102.02-B) and deposited to the Main Cashier's Office.
2. 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.
3. 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):
  - a. 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.
  - b. The storage and inventory of blank receipt stock must be handled by someone other than a cashier.



### **Voids and Refunds**

1. 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.

### **Requirements of Checks Received**

1. All checks must be payable to, California State University, Stanislaus, Stanislaus State University, CSU Stanislaus, CSUS, California State University, Stanislaus Foundation, University Student Union (USU) of California State University, Stanislaus, Associated Students, Inc. (ASI), California State University, Stanislaus Auxiliary & Business Services (ABS) or reasonable variations thereof.
2. Checks accepted by the University must contain all legally required elements including:
  - a. 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.
  - b. Legible and consistent amounts, both the numeric and written.
  - c. Valid signature by the account holder.
3. The following procedures should be followed for checks that do not contain all the legally required elements noted in section 2 above:
  - a. Checks received in person from the payer should be reviewed at the time of receipt for the required elements noted in section 2. If any of the required elements are not met, the cashier must return the check to the payer for correction.
  - b. Checks received in the mail from the payer should be reviewed at the time of receipt for the required elements noted in section 2. If any of the required elements are not met, the cashier should make every effort to contact the payer to request a new check be issued. The cashier should mail the invalid check back to the payer, if possible, otherwise shred the check.
4. 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.
5. 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.

### **Deposits**

1. 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.
2. Deposit counts shall be verified by a second person. For departmental deposits, all deposits will be verified by the main cashier's office.
3. 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





CALIFORNIA STATE UNIVERSITY

Stanislaus

restraints, other compensating controls should be established through consultation with the Cash Handling Coordinator.

4. Satellite cashiering location collections should be deposited within two working days of receipt to the Main Cashier's Office, and supported by a completed Deposit Transmittal Sheet, CASHNet Summary Report, or Audience View Report. Collections made by the Main Cashier's Office should deposit directly to the bank the same day as they are received, or at a minimum, on the following business day.
5. Transporting of deposits should be in a sealed, tamper evident non transparent money bag with a copy of the transmittal retained by the originating office.
6. Transporting of deposits between cashiering stations or to a bank should be accomplished in a secure manner. In order to protect the financial assets and individuals involved, the transport of all deposits shall be accomplished jointly by at least two employees.

#### **Single Cash Transaction > \$10,000**

1. 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.

#### **Security of Cash Funds**

1. The following are the requirements for storage of cash:
  - a. Up to \$1,000 in a lockable receptacle
  - b. \$1,000 to \$2,500 in a safe
  - c. From \$2,500 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.
  - d. From \$25,000 to \$250,000 in a class TL-15 composite safe or better.
  - e. Over \$250,000 in a class TL-30 steel safe or better.
2. Physical security systems are required in areas where large amounts of cash are collected
  - a. 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.
  - b. 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.

#### **Safes/Lockable Receptacles**

1. 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.
2. The order, delivery from vendor, and delivery and installation of safe to the department are the responsibility of the University Locksmith.





CALIFORNIA STATE UNIVERSITY

Stanislaus

3. Safes should be bolted to the ground or wall and such activity must be coordinated through the University Locksmith.
4. The relocation or removal of existing safes must only be performed by the University Locksmith.
5. 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.
6. 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.
7. 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.
8. 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 Cashiering & Cash Management to provide notice of a safe access change.
9. 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.
10. The combination should be known to as few persons as possible consistent with operating requirements and the value of the cash or documents.
11. 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.
12. 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.

#### **Door Combinations**

1. 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".

#### **Securing Against Unauthorized Bank Accounts**

1. 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.
2. 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.



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

<b>Approval and Revision History Approved by</b>	<b>Title</b>	<b>Date Approved</b>	<b>Effective Date</b>	<b>Version</b>	<b>Description of changes</b>
Darrell Haydon	VP B&F	1/12/2017	10/01/2016	1.0	Initial Release





# REQUEST TO ESTABLISH/MAINTAIN CASHIERING COLLECTION POINT

Form-3102.02-A v 1.0

**Submission:** Submit this form to Financial Services no later than June 1<sup>st</sup> each year to obtain approval from the Chief Financial Officer to collect cash, checks, and credit cards for each new fiscal year beginning July 1<sup>st</sup> and ending June 30<sup>th</sup>.

## SECTION A. (General Information)

Type of Request:  New or  Renewal/Modification Effective for fiscal year:

Department Name:

Cashiering Collection Point Location:

Department Responsible Person (DRP):  Phone:   
Email:

Describe the goods, services, and/or donation for which you will receive payments. Please be specific:

Describe security arrangements for cash collection point (i.e., locked cash box, cash register, safes, etc.):

Expected frequency of collections:  Daily  1-2 times a week  3-4 times a week  One Time Event  Other (describe): \_\_\_\_\_

Avg. \$ per frequency:  \$0-\$99  \$100-\$249  \$250-\$499  \$500-\$999  \$1,000-\$2,499  > \$2500

Will debit/credit card payments be accepted at this cash collection point?  Yes  No  
If yes, complete Section B. If no, skip to Section C.

***SECTION B. (Credit Card Processing Information)***

How will you accept credit cards?       In-Person       Internet/eCommerce       POS Software  
     Telephone       Mail       Fax

Debit/credit card acceptance methods (check all that apply):

- Cardholder data is swiped through a standalone, dial-out payment terminal which is **NOT** connected to the internet or to any other system within the environment such as CashNet, Vendini, or Fusion.



Make and model # of payment terminal(s):  How many?   
 Make and model # of payment terminal(s):  How many?   
 Make and model # of payment terminal(s):  How many?

- Cardholder data is swiped through a wedge device connected to the computer that inputs the cardholder data into the payment software application OR the cardholder data is manually input into the payment software application such as CashNet, Vendini or Fusion for payment processing. If so, how many computers use this?



- Cardholder data is obtained using imprint machines and submitted to the Cashier's Office for payment processing.



- Cardholder data is obtained or written manually on paper documents and submitted to the Cashier's Office for payment processing.



- Cardholder data is obtained or written manually on paper documents and entered into an electronic format for printing (i.e. Excel/Word) and hardcopy of cardholder data is submitted to the Cashier's Office for payment processing.

- Cardholder data is NOT obtained, the customer enters their cardholder data directly into an internet based eCommerce webpage payment application.

Please indicate payment application used:

CashNet     Other (i.e. Vendini, etc.) (Describe):

- Other (Describe):

Please indicate the *estimated* annual dollar volume and number of transactions for each applicable credit card acceptance process noted below:

In Person	\$ <input type="text"/>	Transaction # :	<input type="text"/>
Mail/Phone/Fax	\$ <input type="text"/>	Transaction # :	<input type="text"/>
Internet/eCommerce	\$ <input type="text"/>	Transaction # :	<input type="text"/>



---

***SECTION C. (Annual Questionnaires)***

---

In accordance with ICSUAM policy 3102.04 Physical Protection of Cash and Cash Equivalents, Risk Management personnel must review the controls of all cashiering locations. Please attach the two forms below to your request form.

Cash Handling Annual Review Questionnaire (Attachment A)

Cash Handling Segregation of Duties Matrix (Attachment B)

---

***SECTION D. (Cash Handling Procedures)***

---

All satellite cashiering stations should submit the procedures that will be used, or are being used, to process payments. The procedures should include:

- Cash receipts collection process
- Deposit preparation and deposit process
- Review and reconciliation process
- Ensure position titles are used to describe who performs specific duties and to describe the individuals who are approving deposits, voids, etc.
- Procedures should be approved by DRP by way of signature

Satellite cashiering stations who have already submitted cash handling procedures, and their procedures have not changed, do not have to re-submit the procedures.

Cash Handling Procedures are attached.

Cash Handling Procedures already submitted and there are no changes to procedures.



# REQUEST TO ESTABLISH/MAINTAIN CASHIERING COLLECTION POINT

Form-3102.02-A v 1.0

## SECTION E. (Signatures and Approvals)

### Signatures:

Department Responsible Person	Signature	Date
Dean/Sr. Director	Signature	Date

*By signing this form, the DRP and Dean/Senior Director acknowledges that he/she understands his/her role as outlined in the responsibilities section of the Payment Card Industry Data Security Standard and the Administration and Finance Cash Handling Procedures and accepts responsibilities for that role.*

Please submit completed form to the Cash Handling Coordinator located in MSR 112A, Main Cashiers. Questions can be directed to the Cash Handling Coordinator via email at [JPhillips@csustan.edu](mailto:JPhillips@csustan.edu) or by phone at (209)667-3241.

### Recommendations for Approval:

Comments:

Cash Handling Coordinator	Signature	Date
PCI Data Authority (if applicable)	Signature	Date

### Approval:

Request Approved:  Request Denied:

Chief Financial Officer or Designee	Signature	Date



## Cash Handling Annual Review Questionnaire (Attachment to Form 3102.02-A)

Cashiering Location:

Department:

*For answers which are "No" to the below ICSUAM requirements, please provide a brief explanation of mitigating or compensating controls which reduce potential loss and risks.*

		Yes	No (explain)
1.	Are segregation of duties setup to ensure that individuals who handle or have access to cash, checks, or credit card information do not: <ul style="list-style-type: none"> <li>• Have access to approve or post journal entries?</li> <li>• Follow-up with accounts receivable collections?</li> <li>• Have the ability to process refunds, authorize or make adjustments to a customer's accounts receivable balance? (ICSUAM 3102.02)</li> </ul>	<input type="checkbox"/>	
2.	Is each cashier assigned a unique user ID, login, and password not accessible by or shared with other individuals? (ICSUAM 3102.02)	<input type="checkbox"/>	
3.	Is each cashier provided with a cash register drawer, a cash drawer insert, or other secure cash receptacle to which only the cashier has access? (ICSUAM 3102.02)	<input type="checkbox"/>	
4.	Does each cashier lock all cash in a drawer or other secure receptacle whenever leaving the immediate area? (ICSUAM 3102.02)	<input type="checkbox"/>	
5.	Is each cash register tape controlled by unique consecutive numbers generated automatically and recorded with each transaction? (ICSUAM 3102.03)	<input type="checkbox"/>	
6.	Does the cash register or point of sale receipt numbering mechanism provide consecutive transaction number control on the tape accessible only to the manufacturer's service representative or appropriate personnel who are independent of that cashiering station? (ICSUAM 3102.03)	<input type="checkbox"/>	
7.	Does the cash register or point-of-sale system produce session closeout audit totals for verification to receipts? (ICSUAM 3102.03)	<input type="checkbox"/>	
8.	Are session closeout audit totals compared to cash collections and reviewed by a supervisor? (ICSUAM 3102.03)	<input type="checkbox"/>	
9.	For cash receipts received through the mail, are the cash receipts opened in dual custody and logged onto the <u>Cash Receipts Mail Log (Form 3102.02-C)</u> ? (ICSUAM 3102.02)	<input type="checkbox"/>	
10.	Are checks restrictively endorsed (endorsement stamp) immediately upon receipt? (ICSUAM 3102.03)	<input type="checkbox"/>	
11.	When account(s) to which a check should be credited cannot be determined, is the check deposited and recorded as uncleared collections? (ICSUAM 3102.03)	<input type="checkbox"/>	
12.	Are voided transactions or refunds documented and approved by the cashier's supervisor? (ICSUAM 3102.03)	<input type="checkbox"/>	
13.	Are in-person payments collected using only cash registers or point of sale receipt systems?	<input type="checkbox"/>	
14.	Is excess cash from each cash register removed from the cash register drawer and transferred to a secure cash handling area/vault? Excess cash is defined as having more than	<input type="checkbox"/>	

## Cash Handling Annual Review Questionnaire (Attachment A to Form 3102.02-A)

		Yes	No (explain)
	what is generally required for daily operations. (ICSUAM 3102.04)	<input type="checkbox"/>	
15.	Are deposits transported in a sealed, tamper evident non-transparent money bag with the tear off slip retained by the originating office? (ICSUAM 3102.04)	<input type="checkbox"/>	
16.	Are at least two employees present when transporting deposits between cashiering sites or to the main cashier's office? (ICSUAM 3102.04)	<input type="checkbox"/>	
17.	When cash is not being used for current operations, are cash receipts secured in lockable receptacles or safes in accordance with section 10.0 "Security of Cash Funds" in procedure 3101.02? (ICSUAM 3102.04)	<input type="checkbox"/>	
18.	If more than \$2,500 in cash is regularly on hand, is a manual robbery alarm system installed that will alert law enforcement? (ICSUAM 3102.04)	<input type="checkbox"/>	
19.	Are safe purchases or the removal of safes coordinated with the University Locksmith?	<input type="checkbox"/>	
20.	Are the safe combinations being changed whenever a person who knows the combinations leaves the department or otherwise does not have an operational purpose for knowing the combination? (Safe Combination Access Listing, Form 3102.02-E) (ICSUAM 3102.04)	<input type="checkbox"/>	
21.	Are new cashiers adequately trained in accordance with University Cash Handling Procedures (ICSUAM 3101.02)	<input type="checkbox"/>	
22.	Is sales tax collected for sales of tangible goods?	<input type="checkbox"/>	
23.	Department employees are not authorized to create any bank or online account to collect monies for University related functions/activities. <input type="checkbox"/> I am NOT aware of any unauthorized bank accounts being used within the department. <input type="checkbox"/> I AM aware of other bank accounts being used within the department. (Please list): _____		
24.	If a third-party collects cash on behalf of my department, the CFO or designee's approval is required. <input type="checkbox"/> I am NOT aware of any third-party collecting cash on behalf of my department. <input type="checkbox"/> I AM aware of a third-party collecting cash on behalf of my dept. (Please list): _____		

I certify I have sufficient knowledge over the cash collection process for this cashiering location to adequately answer the above questions, and have answered them to the best of my knowledge.

DRP Name (Print)

Title

---

DRP Signature

---

Date

<b>Office Use Only:</b>	Reviewed by: _____ Cash Handling Coordinator	Date: _____
	Reviewed by: _____ Risk Management	Date: _____



**CASH HANDLING SEGREGATION OF DUTIES MATRIX  
(ATTACHMENT B TO FORM 3102.02-A)**

Cashiering Location:	DRP Signature:	Date:
----------------------	----------------	-------

	Cashier	Cashier Supervisor	Employee Name <i>Position</i>	Employee Name <i>Position</i>	Employee Name <i>Dept. Supervisor</i>	Main Cashier's <i>Office</i>	Cash Handling <i>Coordinator</i>	Financial Services <i>General Accountant</i>	Financial Services <i>AVR Accountant</i>	University <i>Controller</i>
<b>CASH RECEIPTING</b>										
<b>Mail Receipting</b>										
• Opens Mail										
• Restrictively endorses mail										
• Lists/logs mail receipts										
<b>Cashier/Lockbox Receipting</b>										
• Handles/Receives Cash										
• Approves refunds and voids										
<b>Other Receipting</b>										
• Process collections for returned checks and ACH									X	
• Process collections for credit card chargebacks						X				
<b>Recording</b>										
• Approves journal entries										X
• Maintains A/R records									X	
• Ability to authorize adjustments to customer receivable										
<b>Depositing</b>										
• Prepares deposit to be sent to Cashier's Office										
• Agrees deposit amount to receipt records (register z-tapes, session audit closeout)										
• Takes deposit to Main Cashier's Office										
• Verifies the departmental deposit counts						X				
• Makes deposit to bank						X				
<b>Reviewing/Reconciling</b>										
• Reconciles deposit receipt records to G/L or posted										
• Verifies total deposit equals the journal entry. Posts JE.										
• Reconciles G/L to bank								X		





## Safe Combination Coordinator Appointment

Form 3102.02-C

Safe Brand:	
Model/Serial #:	
Department Name:	
Location of Safe (Building & Room #):	

### Appointment and Responsibilities of a Safe Combination Coordinator

- The appointment of the Safe Combination Coordinator is approved by the respective Senior Director or Dean. Only a duly appointed Safe Combination Coordinator shall have authority to request to have a safe combination changed.
  
- The Safe Combination Coordinator is authorized to request a safe combination change when conditions warrant a change. A change in a combination code (key) is to be made whenever there is a change in the existing list of personnel having access to a safe, due to a change in employment, new assignment, vacation, sick leave or other reason.
  
- The Safe Combination Coordinator communicates the code only to an authorized code recipient. A code recipient is generally a Cash Change Fund or a Petty Cash Custodian.

<b>Certification of Safe Combination Coordinator:</b>		
<i>I agree to accept custodianship of the safe combination.</i>		
Combination Coordinator's Printed Name:	Combination Coordinator's Signature:	Date:
<b>Approved:</b>		
Senior Director/Dean's Printed Name:	Senior Director/Dean's Signature:	Date:

<b>Office Use Only:</b>		
Copy of Form forwarded to University Controller? <span style="float: right;">Yes</span>		
<b>Safe Combination provided to Safe Combination Coordinator by:</b>		
Locksmith's Printed Name:	Locksmith's Signature:	Date:



# Safe Combination Access Listing

PRINT

CLEAR

Form 3102.02-D

Safe Brand:		
Model/Serial #:		
Department Name:		
Location of Safe (Building & Room #):		
Safe Combination Coordinator:		
Combination Change Date:		
Reason for Combination Change:		
<b>Safe Combination Provided by Locksmith:</b>		
Locksmith's Printed Name:	Locksmith's Signature:	Date:
<b>Acceptance of Responsibility by Combination Coordinator:</b>		
Combination Coordinator's Printed Name:	Combination Coordinator's Signature:	Date:

The Locksmith will send a copy of this completed form to the University Controller.

### Individuals with Access to Safe

The above named Combination Coordinator is required to maintain the following list with the names of individuals who have access/knowledge to the current safe combination.

Whenever an employee of the cash handling unit separates from the unit or the University, the safe combination must be changed and a new form shall be completed with an updated list.

Name of Individuals w/ Access	Signature	Date