Department Of Psychology Cash Handling Policy and Procedure
FY2015
Dr. Suzanne Kieffer, Dir. Admin Academic Affairs

FY2015

OVERVIEW

In accordance with MAPP 05.01.01, Cash Handling is all cash transactions involving the University of Houston, and its colleges. Departments are subject to all applicable state laws and regulations and the governance of the University of Houston policies and procedures, including University of Houston System Administrative Memoranda 03.A.07, – Petty Cash Procedures, 03.F.01 – Gift Acceptance, and 03.F.04 – Cash Handling. Employees of the University of Houston have accountability to the governance of the University safe cash handling practices. Procedures are designed to provide transparent and safe processing for monies received in accordance with accepted standards of internal controls. All employees of the College/Division are responsible for complying with the policies and procedures as described below.

DEFINITION OF CASH

Cash is U. S. currency (dollars and coins); personal, business, bank, and cashier's checks; money orders; travelers' checks; or foreign drafts (but not foreign currency).

POLICY STATEMENT

Employees handling cash are subject to all provisions outlined herein based on MAPP 05.01.01 – Cash Handling. University positions with cash handling or fund custodial responsibilities are designated as security sensitive.

Cash is not to be accepted or disbursed by University employee(s) unless that employee(s) are authorized by the College/Division Business Administrator to handle cash for a specified purpose. All employees authorized to handle cash must be certified annually. This certification is done by completing the online training for Cash Handling. Employees can register for this course at the following website, http://www.uh.edu/adminservices/training/financeonline.htm.

Procedure - Department of Psychology

The Department of Psychology receives cash for clinic services and graduate applications fees. In addition, the department provides cash advance for research projects in the department. Following is a detailed explanation of the department's cash handling procedures in all areas.

Clinic

For the clinic, the client submits payment to a clinic therapist. The therapist gives the client a pre-numbered multi-carbon receipt. The clinic program manager Amy Petesch prepares the general cash receipt and submits it to the department fund custodian, Sharon

Terrell, Financial Coordinator. The fund custodian will make copies of the checks; attach a running tape of cash received, and a copy of the receipt. The checks are restrictively endorsed "For Deposit Only, University of Houston, Department of Psychology." Ms. Terrell then places the general cash receipt and the cash in a numbered sealed bank bag. She also fills out a money transmittal form to record the number of the bank bag and the date that the cash was received. The money transmittal form is attached to the department's copy of the general cash receipt journal. Ms. Terrell then calls the UH Police to request a money pickup. The police officer will deposit the funds in the Bursar's office.

Academic Office
Payment for graduate application fees are received by mail. The academic office staff prepares the general cash receipt and submits it to the department fund custodian. The fund custodian will follow the same procedures/processes as stated in the above section.

Safekeeping
If the fund custodian receives cash after 3 P.M., the cash is locked in a safe in room 128F. (There is no money pick-up after 1:30 P.M.)

Recording of Revenue
The fund custodian keeps an electronic receipt log of all cash received in the department.

Review and Reconciliation
The Department Business Administrator (Ursula Ollivierre) conducts a line-by-line reconciliation of all cash received for the clinic account and the graduate application fee account on a monthly basis.

Cash Advance Procedures:

General Process

- At least 10 days prior to an assessment period, a "Cash Advance" form application is submitted for approval by the Exec Dir., College/Division Business Op, Dean Liberal Arts & Social Sciences. Once approved, a purchase voucher indicating the number and total amount of payments anticipated for a specified assessment period is prepared by the department. The voucher is submitted to Student Financial Services (SFS), who will fill in the appropriate SFS general ledger account number. Special handling will be noted on the face of the voucher. The department address will be listed as the vendor or custodian address.
- Based on the voucher amount, a cash advance check, payable to the fund custodian, is issued by Student Financial Services. The "custodial check" is sent to the department office. The fund custodian records the check number, check amount, and other pertinent information on an internal document called the 'Operational Cash Advance Voucher Closure Form' (see Forms and Record keeping section). When the fund custodian cashes

the check, the department will call UH Police and request a money escort who will walk with the fund custodian to the bank and back to the department.

- Upon completion of assessments a list of all subject payments and a copy of the Operational Cash Advance Voucher Closure Form is uploaded to the closeout Journal which is entered into workflow, charging the project supported, and crediting Accounts Payable "Cash Advance Cost Center". Any unused cash is then returned to SFS by a UH police officer.
-

This cycle would be repeated throughout the duration of the project. Again, because of the nature of the subject population, the "voucher assessment period" may be defined as two week to three month periods. Operational cash advance amounts may range from $1,000 to $5,000 per request depending upon assessment opportunities.

Fund Custodian Designation

The fund custodian for the department is Sharon Terrell the Financial Coordinator. Ms. Terrell is responsible for the safekeeping of the funds and ensuring that the moneys are distributed to the research project team members. As fund custodian, she ensures that funds are expended and accounted for in accordance with MAPP 5.01.02. Undistributed funds are kept in a locked safe in room 128F Heyne building. Room 128F is within a suite that is locked when none-attended. In addition, room 128F is locked after hours. There are only four individuals in the department who have key access to this room. Access to the safe is restricted to the following office employees: Ursula Ollivierre, Sharon Terrell and Dr. Suzanne Kieffer, Director of Admin & Academic Affairs.

Segregation of Duties

EXPENDITURE DOCUMENT PREPARATION, INTERNAL RECORD KEEPING

All voucher preparations for cash advances, subject payment disbursements, and other related documents are prepared by the financial coordinator, Ms. Sharon Terrell. As fund custodian, Ms. Terrell also issues currency to project team members as requested. The fund custodian maintains records of disbursements from the check using the 'Check Disbursement Log'. The log contains information regarding who, when, and how much currency was issued. Ms. Terrell conducts overage/shortage audits a minimum of once a month.

PARTICIPANT PAYMENTS

Prior to disbursement of cash payments to research participants, project researchers collect subject information as required in MAPP 5.02.04. It is the responsibility of the researcher(s) to collect the required information on the 'Payee Certification Form', ensure the safekeeping of currency released to them by Ms. Terrell for disbursement to subjects, the 'Payee Certification Form' is then returned to the financial coordinator by the end of each assessment period. In addition, the project researchers issue a pre-numbered receipt to the payee. A copy of the receipt is attached to the 'Payee Certification Form'.

REVIEW AND RECONCILIATION

Ursula Ollivierre' oversees and reviews the preparation of cash advances, subject payment disbursements records, and other related document preparation. Ms. Ollivierre' conducts a line-by-line reconciliation of the subject payment records to PeopleSoft, and reconciles the fund expenditures on a monthly basis. Records used to reconcile to the PeopleSoft records include the receipt, 'Check Disbursement Log', 'Operational Cash Advance Voucher Closure Form', 'Payee Certification Form', 'Human Subject Payment Record' and the department's internal tracking system.

As certifying agent for the department, the department business administrator ensures that any expenditure are made for the purpose for which the funds were budgeted, that the procurement of all cash advances and all corresponding documents are in accordance with applicable guidelines, that the funds required are available, and that fund reconciliation is conducted on a monthly basis.

Forms and Record Keeping

Attached are four documents developed for of this project.

FORM/RECORD NAME	DESCRIPTION
(A.) Check Disbursement Log	This log is kept and maintained by the fund custodian and is used to record currency disbursements to the researchers.
(B.) Payee Certification Form	This form is used by the researcher to acquire necessary subject data information and payment receipt acknowledgment. These forms are returned to the department with any remaining currency after a determined number of assessments have been conducted, and no less than once every three months. Information from this form is logged into a 'Human Subjects Payment Record' spreadsheet. The 'Payee Certification Form(s)' and any remaining currency is returned to Student Financial Services.
(C.) Receipt	Pre-numbered multi-carbon receipts will be used by the project researchers. Receipts are issued to the payees. A copy of the receipt is attached to the 'Payee Certification Form'.

(D.) Human Subjects Payment Record

This is for internal record keeping control. The spreadsheet can be sorted by name or social security number. If a subject should receive $600 in a calendar year, our department will notify Finance and Accounting. It also provides additional back-up documentation.

(E.) Operational Cash Advance Voucher Closure Form

This form will be used to ensure that the total subject payment disbursement plus any remaining currency equal the amount of the check issued to the fund custodian. This form will be attached to the 'Payee Certification Form(s)' and delivered to Student Financial Services with any remaining currency.

The procedures and forms described above will be audited at least annually by the department. When required, they will be amended to reflect institutional and/or research guidelines or needs.

Copies of MAPP 5.01.02 - Operational Cash Advances and MAPP 5.02.04 - Payments to Human Subjects and Participants in Sponsored Projects, MAPP 5.01.01 - Petty Cash, Cash Funds, and Cash Handling were provided to project team members.

Introduction

This document contains the Department of Psychology policies, procedures, and best practices for daily operations and safeguarding confidential information from unauthorized access and misuse.

Department of Psychology Policy, Procedure and Best Practices builds on federal and state law, University of Houston System Administrative Memorandum 03.A.06 (UH SAM), and University of Houston Manual of Policy and Procedure 05.01.01 (UH MAPP) and should be viewed as a detailed version of these governing laws, policies and procedures. If a conflict exists, authority cascades in this order: Federal law>State law>UH SAM>UH MAPP> Department of Psychology Policies and Procedures. All employees should familiarize themselves with SAM 03.A.06 and MAPP 05.01.01 as we are required to adhere to these policies when handing cash/credit card transactions.

The Department of Psychology is authorized to receive customer payments in the form of cash, checks, money orders, and electronic funds transfer under UH MAPP 05.01.01.

The Department of Psychology is authorized to receive and electronically process customer credit card payments according to the policy and procedure established in UH System Administrative Memorandum 03.A.06.

No one may handle or access credit card numbers or other confidential payment information held by The Department of Psychology without being an employee who is an authorized cash handler of the Department of Psychology.

The Department of Psychology authorized staff accepts credit card payments from customers for clinic services, graduate applications fees, and related services as part of day-to-day business operations. Much of this policy and procedure document is dedicated to safe and secure handling of confidential data and to maintaining secure systems for credit card processing.

The Department of Psychology uses requirements established by the Payment Card Industry (PCI) Data Security Standard Version 2.0 to govern credit card security. The Department of Psychology collaborates closely with the Office of the Treasurer and UH IT Security to comply with the PCI standards. In situations where it is not possible to strictly adhere to the PCI standards, The Department of Psychology establishes compensating controls that meet or exceed the requirement.

The contents of this document are designed to:

- Ensure safety for our staff and customers.
- Protect funds and customer credit card numbers collected by The Department of Psychology from theft, misuse, and unauthorized access.

- Ensure accurate and transparent financial reporting, in accordance with UH MAPP.
- Comply with the PCI Data Security Standards.
- Safeguard sensitive and confidential information from theft, misuse, and unauthorized access.
- Encourage thoughtful and effective customer service.

- This document includes:
- Description of how The Department of Psychology uses Bank of America Merchant Processing UH's secure computing environment for credit card processing.
- Policy and procedure for classifying, handling, storing, retaining, and destroying data.
- Roles, responsibilities, and access authorizations for The Department of Psychology staff who use credit card data and credit card processing systems.
- Policy and procedure for fundamental business operations to ensure that the Department of Psychology is using best practices to mitigate risk of theft, misuse, and unauthorized access to credit card data.
- Electronic security incident response plan.

Employees must make sound judgments regarding security, and credit card processing when necessary. If you encounter a situation not addressed in this document, consult your supervisor or the Department Business Administrator if one is available. If one is not available, use your judgment to solve the problem, and then document your actions and brief the supervisor or business administrator at the earliest opportunity.

In determining a course of action, consider the following priorities which are listed in order of importance:

- Personal safety of staff and customers
- Accurate and transparent accounting of cash and other payments
- Protection of our customer's personal and confidential information
- Thoughtful and effective customer service

The contents of this document pertains only to the Department of Psychology business operations, and credit card processing system components that is based in the Department, and which support the sale of its programs and related services. The department does not cover activity of other groups or other entities at UH that may also be processing credit cards under a different merchant identification number.

Authorized uses of credit card numbers and cardholder data, *Credit card handling and transaction processing*

Credit card numbers may be used by authorized cash handlers to carry out sale or credit transactions, and related products or services for the Department of Psychology. The following guidelines shall be adhered to by the Department staff:

- The Department of Psychology authorized cash handlers may retrieve credit card numbers from the university's merchant bank reporting system as needed to issue transaction voids or credits.
- All other uses of credit card number or cardholder data are prohibited.
- After a transaction is validated, credit card numbers that appear in card processing applications should always be masked except for access by authorized users.
- Complete credit card numbers or any portion of the expiration date or the card verification value (CVV) code must not appear on electronic or printed receipts.
- The Department of Psychology does not store card verification value codes, magnetic stripe data or customer PINs to process transactions. Storage of this data is strictly prohibited for all staff. Credit card numbers must never be stored after a transaction is validated. Credit Card numbers on paper records must be rendered unreadable before being stored. To dispose of paper records that contain credit card numbers, shred them in a cross-cut shredder or place them in a locked shred bin. Authorized users may never save credit card numbers on their computer or in their files.
- Credit card numbers must always be encrypted during transmission among credit card processing systems, if we are not using the bank hosted site provided by the university.

Credit card handling and transaction processing

Credit card numbers may be provided by customers to staff over the phone, in person, or on paper registration forms. In the case of paper registration forms sent through the mail, The Department of Psychology MAY NOT ask for the CVV code on the credit card. The Department cash handlers may retrieve a credit card number used for a past transaction from the processor in order to issue a credit or refund.

The following requirements apply when receiving payments by credit card:

- Check to see that the credit card is signed by the account holder (card-present transactions only).
- Check a second form of government issued identification (e.g. driver's license) to confirm that the person presenting the card is the cardholder (card-present transactions only).

- Swipe or key-enter the credit card number presented for payment directly into the card processing device and validate the transaction immediately.
- Issue a numbered receipt to the customer. Make sure the receipt only prints the last four digits of the customer's credit card number.
- Verify that the credit card number is not stored electronically or on paper after the transaction is validated.
- Credit card numbers retrieved from the processor for the purpose of issuing a credit or refund must be entered directly into the card processing device and processed immediately.
- If a paper record must be stored, the credit card number should be blacked out and the page photocopied. Only the copy may be stored.
- The Department of Psychology will check paper files once per month to ensure that no readable credit card numbers are being stored.

Employees may not:

- Access full card numbers in card processing applications unless there is a legitimate business need to do so and only then by employees authorized by the manager of the department.
- Store credit card numbers in any paper or electronic medium except as specifically allowed by this policy for offsite events, if applicable.
- Store credit card numbers at their desks, on computers, or on removable electronic media (ex. CDs, flash drives, etc.).
- Send or receive credit card numbers via email or email attachments
- Give credit card numbers to a third party, with the exception of the Department of Psychology credit card acquirer/processor.
- Release credit card numbers to any customer, including a person stating s/he is the cardholder
- Release credit card numbers to another UH employee who is not an authorized Department of Psychology cash handler, and who has a legitimate business purpose for needing such information.
- Collect CVV codes printed or embossed on cards, magnetic stripe data, or customer PINs
- Retain credit card numbers in system or application audit logs.

Accepting customer payments offsite

- **General policies**

The Department of Psychology may use the following to process credit card payments at off-site events:

- Paper registration forms, with fields for credit card data located at the bottom of the page where it can be easily cut off.
- Point-of-sale swipe terminals that use a phone connection to the credit card acquirer/processor.
- Other devices or connections if approved by the Office of the Treasurer and UH IT Security.

- **Custody & Security**
    - Credit card numbers, and any other equipment and supplies used to document or secure payments, must be in the custody of the Department of Psychology authorized cash handler at all times. Custody must be documented in a written log. This includes transport to and from the site and while at the site. Storage of these items while at the remote site is not permitted.
    - Validations should take place within one business day of the end of the event.
    - Credit card numbers in paper records should be rendered unreadable as soon as the transactions are validated.
- **Transportation**
    - Electronic or paper records that contain credit card numbers are only allowed outside the Department of Psychology office for transport directly to and from an offsite event and for the duration of that event each day.
    - These items must be returned directly to the Department of Psychology office immediately upon completion of payment activities at the remote site each day.
    - Employees transporting these items between the Department of Psychology office and the remote site must travel point-to-point with no stops.
    - These items may not be left in a vehicle unattended, even if that vehicle is locked.
    - These items may not be stored overnight at a remote site.
    - Upon returning to the Department of Psychology office, records containing credit card numbers must be stored in the department’s safe or equivalent locked device until credit card transactions are validated.

- **Using paper registration forms**

  When paper records are used for off-site registration:

  - Only the Department of Psychology authorized cash handlers may handle registration and payment forms that contain card numbers.
  - Registration forms that contain card numbers must be deposited into a locked box through a slot in the top.
- Keep a written log of when individual cash handlers take custody of registration/payment forms and the locked document box.
- Upon receiving a paper registration form with a credit card payment:
  - Process the credit card transaction through the credit card processing terminal.
  - Immediately when registration activity ends at the off-site event, the locked box of registration forms must be transported directly to the Department of Psychology office.
  - At the Department of Psychology office, forms may be retrieved from the locked box, and transactions not yet processed may be processed through the credit card processing terminal.
  - If paper records containing credit card information, the records must be stored, those must be enclosed in a clearly labeled envelope in the safe, or equivalent locked device, in the department.
  - All transactions must be processed within one business days of the off-site event.
  - Credit card information on registration forms must be cut off and shredded or deposited in a locked shred bin immediately after the transaction is processed. The rest of the form may be retained if needed.

Opening mail

Mail delivered to the Department of Psychology sometimes contains credit card payments. Any mail addressed to the Department of Psychology or addressed to our office without an individual’s name must be opened by the Department of Psychology authorized cash handler.

Typically, the cash handler designated to open mail will be someone whose daily responsibilities do not normally include payment processing.

Once a payment is received by mail, the person who received it will hand it off to a cash handler who normally accepts payments, and that individual will process the payment immediately.

Physical security of work and storage areas

The Department of Psychology work and storage areas include the Department of Psychology and its Clinic. These are security-sensitive areas where cash and confidential information are stored.

Visitors may not be left unattended in any area of the Department of Psychology. When the office is open, visitors must be accompanied by an authorized cash handler for the Department of Psychology.

Doors to the Department of Psychology must be locked when the office is closed and staff is not present. If staff must leave the area during business hours, these doors will be locked and signs posted directing visitors how to contact a staff member.

Credit card swipe terminals used to process credit card transactions that are in reach of the public must be visible to our staff at all times. Whenever the office is unoccupied, the doors, in which credit card swipe terminals are located, must be locked. At the end of the day, credit card swipe terminals must be stowed outside public view, if not secured to a counter, for example, and the door(s) to the office area in which the credit card swipe terminals are located must be locked.

All applications open on computers must be closed, and the user logged off the computer before leaving the computer. At the end of the day, the computer should be turned off. Both of these actions mitigate the risk of unauthorized access to this device used to process credit card transactions.

Clean desk policy

Each employee’s work area and desk are security sensitive zones where sensitive and confidential information may be stored. Sensitive and confidential information should not be visible on staff desks except when the individual is working with it.

When walking away from your desk temporarily:

- Scan your work area for sensitive or confidential records and store them out of sight.
- Lock your computer desktop so that a password is required to unlock it.
- When leaving the office for any length of time:
    - Scan your work area for sensitive or confidential records and store them in a locked drawer or safe.
    - Turn off your computer desktop.

Using email

Email is not a secure form of communication. Always assume that unencrypted email and attachments can be read by anyone. The following guidelines will be followed by our staff:

- Do not send sensitive information via unencrypted email.
- Never send confidential information via unencrypted email.
- Never send PCI data via email under any circumstances.
- Do not distribute personal and sensitive information to persons who do not have a legitimate business purpose for having it.

Receiving credit card data via Fax

Cardholder data can be received via fax provided the following conditions are met:

- Fax machines must be stand-alone fax machines. Fax server accounts cannot be used to receive credit card data.
- Fax machines must be physically secured against unauthorized access. Cardholder data is susceptible to unauthorized viewing, copying or scanning if it is unprotected.
- If a transaction cannot be validated immediately, the record may be stored in the safe for up to 1 business day while you gather information or re-attempt validation. After one business day, the record must be securely destroyed as described in this policy.

Cash and credit card handling training program

The Department of Psychology supervisor will ensure that cash handlers are cleared through a criminal history background check and receive thorough training in credit card security policy and procedures.

Employees with access to credit card data must sign a statement to acknowledge in writing that they have read and understand the department’s security policies and procedures.

Training

New hire training and annual recertification of university approved online webinars for credit card processing must be successful completed by the university’s established deadline in order to begin or continue processing credit cards. The currently approved list of courses is as follows:

- UH Credit Card Processing
- UH Credit Card Data Security

- UH Data Security Training

In addition, the supervisor will review each component of the Department of Psychology policies, procedures, and best practices relevant to cash handling and credit card processing with its employees periodically.

Each employee must sign a statement confirming that s/he has read and understands the department's policies and procedures, especially the following:

- His/her responsibilities
- The reasons for the security policies
- The Department of Psychology best practices for securing cardholder data
- Proper step-by-step procedures for job duties that require access to cardholder data
- Consequences for non-compliance
- Procedures for reporting irregularities and violations

PCI Data - Description

- PCI data include:
- Credit card numbers
- Card verification values (CVV and CVV2)
- Magnetic stripe data
- Customer PINs
- Passwords and access codes used to access confidential data, PCI data, and systems that contain such data
- SSL certificates

Handling PCI Data

By this policy, for each type of PCI data, the Department of Psychology employee must be authorized to access or handle that data. If this policy does not include, then separate, written authorization must be approved by the Department of Psychology management. The employee must in a position classified by the university as security sensitive and have a business need for the data before authorization will be granted.

PCI data must always be encrypted with 128-bit encryption compliant with the PCI Data Security Standard while in transmission.

Employees may **NOT**:

- Use PCI data or other data for any purpose except those described in this document.

- Store credit card data in electronic or paper records, except in the limited circumstances allowed by this document for un-validated transactions or paper records collected at offsite events.
- Send or receive PCI data via email or email attachments.
- Access full credit card numbers except when there is a legitimate business need to do so.
- Give PCI data to a third party. As the sole exception, credit card numbers may be given to the Department of Psychology credit card acquirer, in order to process or research a transaction for the Department of Psychology.
- Release PCI data to any customer, including a person requesting a credit card number and stating s/he is the cardholder.
- Release credit card numbers to another UH employee who is not an authorized Department of Psychology cash handler and who has a legitimate business reason for having such sensitive information.
- Collect or store verification numbers printed or embossed on cards, magnetic stripe data, or customer PINs.
- Print or export reports that contain full credit card numbers.
- Use real credit card numbers in test transactions.

Audit

The Department of Psychology supervisor will audit paper files and the department safe periodically but no less than quarterly to make sure no forms or receipts with credit card numbers are being stored, and document this audit in a log.

Quick Reference: How to report problems

What should I report?

- Cash handling irregularities
- Suspected policy violations
- Security incidents

When do I use the Incident Response Plan?

Ask yourself these questions:

- Does the irregularity or violation pose a danger to staff or customers?

- Does the irregularity or violation have potential to disrupt regular business operations?
- Could the irregularity or violation put customer credit card numbers or other confidential and PCI data at risk for unauthorized access or misuse?

If the answer is “yes” to any of them, you must trigger the Department of Psychology Incident Response Plan. The plan includes instructions on how to report the problem.

How do I report a problem without using the Incident Response Plan?

You may choose one of these responses:

- Report the problem to the supervisor, the Department Business Administrator, or a higher authority in the Department of Psychology
- Follow the instructions to report fraud or suspected fraud in UH System Administrative Memorandum 01.C.04
- Report the problem at MySafeCampus.Com

  MySafeCampus.Com allows any UH employee to report policy violations and provides a way to do so anonymously if you desire.

Department of Psychology Incident Response Contact List

Updated Ursula Ollivierre 07/29/2014

Incident Response Contacts	Name/Title	Office	Cell	Email
Department of Psychology Supervisor	Suzanne Kieffer	126 Heyne Building	713-743-8504	kieffer@uh.edu
Department of Psychology Management	Amy Petesch	1000C CRS	713-743-1747	alpetesch@uh.edu
Emergency		911		
UH Campus Police Non-Emergency		713.743.3333		

Other Key Contacts				
Department Business Administrator	Ursula Ollivierre	126 Heyne Building	713-743-8597	ursulam@uh.edu
Card Processing Device Tech Support				
UH IT Security	Mary Dickerson	832-842-4679		medickerson@central.uh.edu
UH Treasurer	Roberta Puryear	713.743.8780		rdpuryea@central.uh.edu