Introduction

This document contains the Center for Public Policy policies, procedures, and best practices for daily operations and safeguarding confidential information from unauthorized access and misuse.

The Center for Public Policy policies, 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, The Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy without being a Center for Public Policy authorized cash handler.

The Center for Public Policy staff accepts credit card payments from customers for 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 Center for Public Policy uses the requirements established by the Payment Card Industry (PCI) Data Security Standard Version 2.0 to govern credit card security. The Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy staff who use credit card data and credit card processing systems.
- Policy and procedure for fundamental The Center for Public Policy business operations to ensure the department is using best practices to mitigate the risk of theft, misuse, or 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 pertain only to The Center for Public Policy business operations and card processing system components based in The Center for Public Policy and which support the sale of The Center for Public Policy programs and related services. It does not cover activity of other groups within The Center for Public Policy or other entities at UH that also may 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 for services. The following guidelines shall be adhered to by The Center for Public Policy staff:

- 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 Center for Public Policy 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. Never save credit card numbers on your computer or in your 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 Center for Public Policy MAY NOT ask for the CVV code on the credit card. The Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy 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 The Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy office immediately upon completion of payment activities at the remote site each day.
    - Employees transporting these items between The Center for Public Policy 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 The Center for Public Policy office, records containing credit card numbers must be stored in The Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy office.
    - At The Center for Public Policy 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 must be stored, they must be enclosed in a clearly labeled envelope in the safe, or equivalent locked device, in The Center for Public Policy safe.
    - 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 Center for Public Policy sometimes contains credit card payments. Any mail addressed to The Center for Public Policy or addressed to our office without an individual's name must be opened by a Center for Public Policy 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 Center for Public Policy work and storage area includes 306 McElhinney Hall. These are security-sensitive areas where cash and confidential information are stored.

Visitors may not be left unattended in any area of 306 McElhinney Hall. When the office is open, visitors must be accompanied by a Center for Public Policy cash handler.

Doors to the 306 McElhinney Hall must be locked when the office is closed and any time staff are 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 Center for Public Policy 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 are 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 Center for Public Policy 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 Center for Public Policy 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

For each type of PCI data, a Center for Public Policy employee must be authorized to access or handle it by this policy. If this policy does not include it, then separate, written authorization must be approved by The Center for Public Policy 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 [*repeated for emphasis*]:

- 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 Center for Public Policy credit card acquirer, in order to process or research a Center for Public Policy transaction.
- 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 Center for Public Policy 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 Center for Public Policy supervisor will audit paper files and The Center for Public Policy 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 Center for Public Policy 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 Center for Public Policy.
- 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.

The Center for Public Policy Incident Response Contact List

Updated 08/08/14 ZKL

Incident Response Contacts	Name/Title	Office	Cell	Email
The Center for Public Policy Director/Supervisor	James Granato	713-743-3887		jgranato@central.uh.edu
The Center for Public Policy Assistant Director	Lauren Neely	713-743-3975		lneely@central.uh.edu
Emergency		911		
UH Campus Police Non-Emergency		713-743-3333		

Other Key Contacts				
Associate Director	Renée Cross	713-743-3972		rcross@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