University of Houston Clear Lake

Credit Card Merchant Identification/ID (MID) Setup and Maintenance Procedures

Statement

This document sets requirements and procedures for the setup and maintenance of a Merchant Identification/ID (MID) for the acceptance of credit card payments for the sale of approved goods, services, information or gifts.

Reasons for this document

The purpose of this document is to set control procedures and requirements prior to the acceptance of credit card payments to prevent loss of confidential data and ensure compliance with university policies and industry security standards and regulations.

Primary guidance to which this document responds

E-Commerce: Electronic Protection of Credit Card Holder Information Policy and to the Payment Card Industry Data Security Standard (PCI DSS).

Responsible University office

UHCL Business Operations and UH Office of the Treasurer.

Who is governed by this document?

This document applies to individuals, colleges, departments, centers, institutes, and programs ("University Departments") that sell goods, services, information, or gifts and accept credit cards as a form of payment.

Who should know this document?

All college/division business administrators, department administrators and financial and administrative staff whose business accepts credit cards as a form of payment should know this document.

Exclusions and special situations

None

Document text

A university department accepting credit card payments for the sale of goods, services, information or gifts is a merchant. In order to accept credit card payments, the merchant must obtain an MID which is a unique number that identifies the merchant for reference and billing purposes.

There are four methods for processing merchant transactions that require an MID:
1. Mail order (ex. Lockbox, card not present);
2. Telephone Order (card not present); } together MO/TO
3. Retail face to face (Point of Sale (POS), card present);
4. E-commerce (internet/computer network, card not present).

University departments must follow guidelines to capture, store or transmit credit card information on UHCL servers or network in a secure manner. Reference SAM 03.A.06 (3.5)

Data Retention

Transaction receipts (paper or electronic records of the purchase) must be retained for a minimum of two (2) years (or such period as the Card Rules or the Laws may require or your specific department guidelines mandate) to dispute a chargeback from a cardholder if necessary. The receipts should be stored in a safe, secure area and organized in chronological order by transaction date and kept locked on site for 2-3 months and then placed in archives for the remainder of the two years. They should be securely destroyed directly from archives.

What is the process for a department to get an MID?

Department/s requesting an MID for their normal daily operations schedule a meeting to discuss their needs with General Accounting and UCT, sharing information with facts and figures to support the departmental daily operational needs. See section 'Department Responsibilities' for additional details to request an MID.

Department Responsibilities

UHCL MID will only be issued to university departments that comply with this document, all related policies and acknowledge technical and operational responsibilities associated with credit card acceptance. All university department merchants must comply with university policies to safeguard credit card and other personally identifiable or sensitive information.

- University departments may ONLY obtain a UHCL MID by submitting a request to UHCL Business Operations for approval with the following information:
  - Determine the need for a merchant account
  - Purpose of the account
  - Annual anticipated dollar and transaction volume
  - Monthly average transaction amount
  - Frequency of transactions (year-round, seasonal, limited)
  - Type of processing required (MO/TO, POS, e-commerce).
  - Request new or update to an existing MID approved by Requester, the College/Division Business Administrator, and the Department Head.
  - Acknowledge review and compliance with UHCL policies and procedures.
  - Complete and submit required forms provided by the UHS Treasurer's office, including New Merchant Account Application and PS account numbers for revenue and expenses.
- Acknowledge understanding of responsibilities of MID User access rights.
- Ensure that cardholder data is treated as confidential and access is restricted to a need to know basis.
- Ensure functional segregation of duties between employees who process credit card transactions and chargebacks with those who balance and reconcile the transactions.
- Ensure departmental personnel are trained not only on UHCL policies and procedures but also local departmental procedures related to authorization of transactions, segregation of duties, reconciliations, chargebacks, record retention, data access, training, and physical security.
- *If processing credit card data via e-commerce*, select an approved third-party e-commerce vendor by coordinating with UHCL Contract Administration.
- If an approved vendor cannot support the business objective, a new vendor may be recommended, but must first be reviewed and approved by Procurement Services.
- General Accounting, a part of Business Operations, is the liaison with UHS Treasury, who approves the issuance of an MID upon completion of an authorized UHS Credit Card Merchant Request Form.

Departmental Ongoing Maintenance Requirements

- Reconcile credit card receipts total (from POS device or online terminal) to credit card cash deposits total (cash deposited into UHCL bank account) daily. This will validate that transactions are correct, that there has not been a keying error and/or any malicious activity.
- Reconcile account activity monthly. It is important to record sales revenue and expense timely and accurately. It is incumbent on the university departments to reconcile PS accounts to ensure that revenue and related expenses are posted accurately. Any discrepancies must be addressed timely.
- Coordinate with General Accounting on questions related to the monthly credit card analysis fees.
- Contact Business Operations to update an MID. Reasons to update an MID include the addition of new website associated with an existing MID or a change to a website associated with a current MID or a change in MID Users or contact person, a change in PS account numbers, or a change in business purposes for which the MID was established.
- Contact Business Operations to close an MID. Reasons to close an MID include unauthorized activity, no activity/dormant or a change in business purpose for which the MID was established.
- Certify compliance with PCI DSS technical and operational requirements as requested by the UH Office of the Treasurer on an annual basis.

UHS OFFICE OF THE TREASURER

- Initial Setup Requirements
  - Obtain authorized approval from UHCL Business Operations of the department MID request.
  - Provide approximate transaction and service fees associated with processing credit cards as well as setup and monthly fees for online merchant accounts.
- Ongoing Maintenance Requirements
  - Review as necessary university MIDs and transactions for compliance with university policies and industry standards and regulations.
  - Recommend MIDs for update or closure. Reasons include changes in the original purpose of the MID, addition of new websites associated with the MID, unauthorized activity, no activity/dormant, the PeopleSoft accounts are not reconciled timely or there are significant unresolved open items, and violation of university policies or industry standards and regulations.
  - Review MID Users access for activity and validity of accounts.
  - Coordinate university department's certification of compliance with PCI DSS technical and UHCL operational requirements on an annual basis.

Consequences for Non-Compliance with this document

Failure to comply with this document can result in the termination of merchant services privileges and individuals may be subject to disciplinary action and/or sanctions up to, and including discharge or dismissal in accordance with university policy and procedures.

Additionally, intentional negligence that results in breach of confidentiality of personal information that is protected by law, acts, or regulations, can also result in criminal prosecution.

Penalties for non-compliance of PCI DSS requirements include fines up to $500,000 per incident if data is compromised.

Respond to a Credit Card Security Breach
If you have knowledge of or suspect a security breach of credit card data, report the incident to:

- Anthony Scaturro, UHCL Information Security Officer at 281-283-2954 or Scaturro@UHCL.edu
- University Information Technology (UIT) Security via the Online Incident Report Form or UHS Office of the Treasurer at (713)743-5670 or lwedwards2@uh.edu
- Mary Dickerson, Chief Information Security Officer and Executive Director of UIT Security, at 832-842-4679 or MEDickerson@central.uh.edu
- You must also take immediate steps to preserve all business records, logs and electronic evidence.

Contacts
For questions or comments
Office of Business Operations AVPBusOps@uhcl.edu or (281)283-2140

Cross References to Related Policies
The University of Houston System Administrative Memorandum, SAM 03.A.06
For more information on PCI, refer to the PCI Security Standards Council. They also maintain a list of approved companies and providers. All processes for accepting credit cards must comply with Payment Card Industry Data Security Standards (PCI DSS). The standards globally govern all merchants and organizations that store, process or transmit credit card data. For additional information refer to PCI Best Practices