SECTION: Fiscal Affairs **NUMBER: 03.A.06**

AREA: General

SUBJECT: Establishment, Maintenance, and Discontinuance of Credit Card Services

---

1. PURPOSE

This document prescribes the standards for the acceptance of credit cards by University of Houston System (UHS) component universities that store, process, or transmit credit card data.

2. DEFINITIONS

2.1. Payment Card Industry Data Security Standards (PCI DSS): A single approach to safeguarding sensitive data for all types of credit cards. This Standard is a result of collaboration between Visa and MasterCard and is designed to create common industry security requirements.

2.2 Acquiring Bank: A bank or financial institution that processes credit and or debit card payments for products or services for a merchant.

2.3 Merchant: For purposes of this policy, any system component department that accepts credit or debit cards as payment for goods or services.

3. POLICY

3.1. Only PCI DSS compliant vendors may be used by the System. Proof of compliance must be in writing from the vendor or other credible source such as Visa. The PCI Security Standards Council also maintains a list of approved companies and providers.

3.2. The UHS Treasurer's Office is:

A. Authorized to negotiate credit card processing and related services on behalf of the System. The System will consolidate credit card processing with one Acquiring Bank in order to take advantage of the negotiating leverage offered to the System by the consolidated credit card transaction volume generated by the System component universities.

B. Responsible for promulgating guidelines for the storing, processing, and transmitting of credit card data to help ensure compliance with the PCI DSS.

C. Responsible for coordinating with UIT Security and the merchant location, in the event of a security breach involving credit card data, a notification to the appropriate entities in accordance with the Credit Card Data Security Incident Response Plan.

3.3. Each Chief Financial Officer (CFO) is responsible for:

A. Ensuring its component university complies with all credit card industry standards, rules or regulations as well as state or federal laws related to credit card acceptance and adherence to this document.

B. Appointing a PCI DSS compliance representative for its component university. The component university's PCI DSS compliance representative is responsible for ensuring that each merchant within its university performs the responsibilities established by the UHS Treasurer's Office.

3.4 PCI DSS compliance representatives are responsible for:

A. Requiring annual training for all staff who currently initiate credit card transactions, access credit card information, prepare credit card journal entries, or supervise staff who perform any of these functions. This training must include information security awareness.

B. Requiring all staff who wish to begin initiating credit card transactions, accessing credit card information, preparing credit card journal entries, or supervising staff who will be performing these tasks, to successfully complete standardized training prior to performing these tasks.

C. Ensuring a system and procedures are in place to monitor and analyze security alerts and information and distribute these alerts to the appropriate personnel.

D. Reporting a system compromise or a suspected system compromise involving credit card data to UIT Security via the Online Incident Reporting Form.

3.5. Merchants are responsible for:

A. Following guidelines promulgated by the UHS Treasurer's Office for the storing, processing, and transmitting of credit card data.

B. Obtaining approval from the UHS Treasurer's Office prior to accepting credit cards in any form, including web transactions through third party processors, using the Credit Card Merchant Request Form.

C. Completing the annual PCI DSS certification.

D. Participating in reviews for compliance with the PCI DSS and UHS guidelines by the PCI DSS Compliance Representatives, UHS Treasurer's Office, UH Information Technology Security Department, and Internal Audit.

3.6 The UH Information Technology department is responsible for maintaining a standardized, secured data network for the initiation and acceptance of credit card transactions.

3.7. Discount fees and other fees and expenses related to accepting credit cards will be charged on a periodic basis to the merchants accepting credit cards. The discount fee and related fees and expenses are variable and subject to re-negotiation periodically.

4. REVIEW AND RESPONSIBILITIES

Responsible Party: Associate Vice Chancellor for Finance

Review: Annually to determine if the PCI standards have changed; otherwise every three years for all other sections of this policy.

5. APPROVAL

Approved: Jim McShan
Interim Vice Chancellor for Administration and Finance

Renu Khator
Chancellor

July 28, 2015
Date

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	08/03/1998	Initial version
2	02/07/2001	Applied revised SAM template. Removed "component" from procedure to emphasize each "university's" responsibility for credit card acceptance and transactions. Removed the MasterCard and Visa exceptions from Section 2.3. Removed MasterCard, Visa, Discover, and American Express exceptions from Section 3.3. Section 4.5 documented leased equipment rules. Removed Section 5.2.f and Section 6.2.g
3	10/16/2007	Applied revised SAM template. Removed all definitions from Section 2.0 except PCI Data Security Standards. Rewrote entire policy to reflect current operating standards, including new Section 3.2 and removal of Sections 3.5, 3.6, 3.7, 3.9, 3.10, 3.11, 3.14, 3.15, 3.19, 3.20, and 3.21
4	05/25/2011	Applied revised SAM template and added new revision log. No additional changes per Subject Matter Expert
5	07/28/2015	Added "Acquiring Bank" to Section 2.2 definitions, and "Merchant" to Section 2.3 definitions. Redefined Data Security Standards as "DSS" throughout text. Provided links to all forms in document. Added PCI Security Standards Council responsibility to Section 3.1. Redefined the responsibilities for the UHS Treasurer's Office (Section 3.2), the Chief Financial Officer (CFO) (Section 3.3), PCI DSS Compliance representatives (Section 3.4) and Merchants (Section 3.5). Added the responsibility of UH Information Technology department to Section 3.6. Removed Sections 3.9, 3.10, 3.11, and 3.12