Texas A&M University – Corpus Christi
Certification of Departmental Credit Card Procedures

Department: _____

Department Head: _____

Business Manager/Coordinator: _____

Purpose

The following procedure defines and outlines proper processing procedures, necessary training, appropriate physical storage and authorized access to credit card data. Please review and sign below that you understand the policy and procedures that must be followed with accepting and handling credit cards on behalf of the university.

Definitions

- **Card Verification Code** or **CVC** is the 3-digit numeric code printed on the credit card, used for additional verification.
- **Sensitive Authentication Data** or **SAD** comprises 1) the CVC, 2) the full track data of any magnetic stripe or chip on the card, and 3) any PINs or PIN blocks.
- **Primary Account Number** or **PAN** is the 12 - 16 digit number on a credit card.
- **Cardholder Data** or **CHD** comprises the PAN, the cardholder's name, the service code, and the expiration date.
- **Media** means electronic or paper records containing any CHD.
- **Merchant** is the person who was granted a Merchant ID by Accounting.
- **Merchant Personnel** comprises the Merchant and any persons authorized by the Merchant to conduct credit card operation's on the Merchant's behalf.

1. Authorized Users (Merchant Personnel)
    a. Only the Merchant may authorize specific persons (Merchant Personnel) to access/use Merchant's Devices, CHD, and Media.
    b. The Merchant shall:
        i. Authorize as Merchant Personnel only those persons who:
            1. Have a legitimate business need for access; (7.1.2, 7.1.3)
            2. Have passed a background check (21.01.02.C0.01, section 2.4.1);
            3. Have taken the required PCI training in the last 12 months. (12.6.1)
        ii. Give Merchant Personnel the least privilege they need to perform their job, and no more.
        iii. Maintain a documented list of Merchant Personnel ("Merchant Personnel List") and update that list when people are added, removed, or have their job duties changed.

1. For each person, the Merchant Personnel List shall list at least name and UIN.

iv. Ensure that Merchant Personnel take PCI training annually. (12.6.1)

2. Protection of Cardholder Data (CHD) and Sensitive Authentication Data (SAD). **If and only if** Merchant Personnel process or record CHD or SAD, electronically or on paper (i.e. Media), then the Merchant shall ensure that:
    a. All SAD is deleted or rendered unrecoverable upon completion of the authorization process. (3.2)
    b. The PAN is masked when displayed or recorded on media such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. (3.3)
    c. PANs are never sent via end-user messaging technologies e.g. SMS text, email. (4.2)
    d. All Media are physically secured. (9.5)
    e. Strict control is maintained over the internal or external distribution of any Media. (9.6)
    f. Media is classified so the sensitivity of the data can be determined. (9.6.1)
    g. Media is sent by secured courier or other delivery method that can be accurately tracked. (9.6.2)
    h. Approval of Merchant is obtained prior to moving the Media (especially when media is distributed to individuals). (9.6.3)
    i. Strict control is maintained over the storage and accessibility of Media. (9.7)
    j. All Media is destroyed when it is no longer needed for business or legal reasons and records retention requirements have been met. (9.8)
    k. Media destruction performed as follows:
        i. Hardcopy materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. (9.8.1a)
        ii. Storage containers are used for materials that contain information to be destroyed secured to prevent access to the contents. (9.8.1b)
3. Devices. **If and only if** the Merchant uses any Devices, then:
    a. Merchant shall:
        i. Maintain a complete and up-to-date list ("Merchant Device List") of all Merchant's Devices listing make, model, serial number, and location for each device. (9.9.1a)
        ii. Update the device inventory whenever a Device is added, removed, relocated, or modified. (9.9.1b, 9.9.1c)
    b. Merchant and Merchant Personnel shall:
        i. Periodically compare the Device inventory to the devices present to see if any devices are missing or have been substituted with other devices. (9.9.2)
        ii. Periodically inspect all of Merchant's Devices for signs of tampering (e.g., broken seals). (9.9.2)
        iii. Be on the lookout for suspicious behavior and validate the identity of any person asking for access to Devices or CHD. (9.9.3)
        iv. Physically secure Devices. Devices that are not being actively used or monitored shall be locked away.
4. Incident Reporting
    a. Incidents are:
        i. Any violation of the policies above;
        ii. Any unauthorized access to CHD, SAD, Media, or Devices;
        iii. Any suspected tampering of Devices or suspicious persons requesting access to Devices or Media.

b. Merchant Personnel shall report incidents to the Merchant. (9.9.3(a))
c. Merchant shall report all incidents to the Office of Information Security at ois@tamucc.edu.

5. Internal Control
    a. Per TAMUCC Procedure 21.01.02.C0.01 "Credit Card Collections, "departments must have standard operating procedures (SOP) in writing that cover use of terminals, forms, reconciling transactions, record retention, training and any other information to conduct business and provide a copy to financial services."

Certification Statement:

I understand that as the chair or head of a department, office, or laboratory that accepts credit or debit cards for any purpose, I am responsible for ensuring that proper procedures for handling and accounting for credit cards are followed, and that cash handling requires special control measures that must be monitored continuously by supervisory personnel to detect any weaknesses. I have reviewed my department's detailed credit card procedures and certify to the best of my knowledge and belief, that they comply with System Policies 21.01.02 Receipt, Custody, and Deposit of Revenues and 21.01.11 Working Funds.

_____ _____

Department Head Approval Date: