TEXAS STATE UNIVERSITY
The rising STAR of Texas

Procedure: Payment Card Acceptance Implementation

As Texas State continues to expand usage of electronic payments, we face new challenges that can potentially expose our customers to unwanted risks and costs. Electronic payment acceptance across campus must comply with the Payment Card Industry Data Security Standards (PCI-DSS) for payment card data protection. In addition to PCI-DSS, policies and contracts are in place at the University, TSUS and state which further regulate electronic payment acceptance. To ensure that the University is in compliance, everyone accepting or considering accepting credit, debit or check cards must adhere to the following:

Only university approved processors or gateways may be used. Processor exceptions must be approved by the Vice President for Finance and Support services and may involve TSUS Board of Regents approval.

- Authorized third-party vendors handling University customer account data may be required to:
  - serve as the merchant of record for processing and PCI compliance
  - transfer funds receipted to University within seven days without direct access to University depository
  - provide PCI related compliance records and attestations
- Customer account data transmitted using University resources must be authorized by Student Business Services, Infrastructure Services, and IT Security. Wi-Fi, using the campus Wi-Fi network, transmission is not permitted.
- PCI Certified Point to Point Encryption technology should be sought out and requested when selecting new payment services vendors or applications, in order to reduce risk and PCI infrastructure requirements.
  - Similar encryption technology, not certified by the PCI Council, must be vetted by Student Business Services and IT Security.
- Customer account data cannot be stored on any Texas State system (POS, kiosks, computers, spreadsheets, databases, SAP, Banner, etc.); therefore, customer account data must not be emailed in any form (scans, call-pilot faxes, etc.) or faxed to a machine (including IKON, Canon, etc.) that is connected to the network.
- Customer account data must not be noted in any form other than paper. Card data should be appropriately redacted and attached to Cashier deposit slips for secure storage and transported securely (in a locked, sealed, or zippered bag or briefcase). Unnecessary copies must not be made or stored. Until deposits are made, or should a department have legitimate need to retain a copy of this information beyond the deposit requirement, it must be kept in a secure environment in a locked area (drawer, safe, cabinet), only accessible to authorized personnel, and cross-cut shredded as soon as no longer needed, but not longer than 2 months. Full card data must not be stored following authorization, and must be appropriately redacted while stored.
- Dial-up terminals and fax machines transmitting customer data must be secured (not easily accessible by public), never left unattended, kept in a secure environment behind a locked area, and settled every evening.
- Authorized payment stations and kiosks must be settled every evening and must not be accessed or transported by non-authorized personnel.

Departments handling any aspect of customer account data must notify Student Business Services in advance for authorization, guidance, and training.

The following procedure outlines the steps to be taken in order to properly vet and implement new payment applications and payment vendors. This procedure should also be taken into consideration when updating existing payment services.

I. Contact Student Business Services for University approved processors, gateways, and vendors for payment processing.
   A. Texas State will utilize payment card terminals provided by the approved, contracted Merchant Processor whenever possible.
   B. If department needs cannot be met by previously approved processors, gateways, and vendors, SBS will assist in looking at other options, which must be appropriately vetted before contracts are signed, and services and systems are implemented.

II. Request For Purchase (RFP) – When appropriate, the RFP process must take place to procure a new vendor for payment processing.
   A. Submit RFP for review by Procurement and Strategic Sourcing to include Texas State University System PCI DSS Addendum, which contains requirements for payment processing as outlined by the Payment Card Industry Data Security Standard.

III. IT Project Management –
   A. Project managers should include the following, as appropriate, in meetings for implementation of payment processing services:
      i. Student Business Services
      ii. IT Security Office
      iii. Network Operations
      iv. Core Systems

IV. Vetting
   A. Appropriate documentation should be collected from the Vendors which may include the following:
      i. Attestation of Compliance for Service Provider
      ii. Attestation of Compliance for PA-DSS
      iii. Point to Point Encryption Collateral
      iv. Data Flow Diagram
      v. Network Diagram
      vi. Higher Education Cloud Vendor Assessment Tool (HECVAT) for Cloud hosted services only
   B. All Stakeholders must approve the account, which may include, but is not limited to:
      i. Procurement and Strategic Sourcing
         1. Complete RFP as applicable
      ii. Electronic Payment Infrastructure Team
         1. Complete the Request to use a Third Party Vendor Application
         2. A risk assessment will be completed with decline for use OR approval with recommendations, and may require a Vice President's signature.
      iii. Information Security Office
         1. Complete the Service Evaluation for new technology.
         2. Will issue decline for use OR a Data Security Plan for implementation.

V. Contracts
   A. When engaging payment service providers, the Texas State University System's PCI DSS Addendum for Service Providers should be included before completing the contract. See Resources for Addendum.
   B. Vendors, and all integration partners, should provide their own PCI Attestations of Compliance, data flow diagrams, and other appropriate PCI documentation.
   C. University Legal will review contracts before appropriate authority signs them.

VI. Implementation
   A. Appropriate time lines should be approved for implementation of all new payment processing services and/or software to ensure proper testing prior to going live. This will ensure a better payment experience for the department and its patrons.
   B. A test environment should be provided by the payment service provider. Application software will be tested in a campus test environment.
   C. All appropriate parties (III.A) must be included in the testing process.

VII. Department PCI Assessment
   A. Departments will be assessed by Student Business Services for PCI compliance upon implementation of their new payment processing service or software.
   B. All department employees involved in payment administration and processing will undergo PCI training prior to accepting payment cards.
   C. Student Business Services will assess Departments on an annual basis for PCI compliance, or after any major changes in the PCI environment.

VIII. Contract Renewals
   A. ISO and the EPI Team will review all renewals of Third Party Contracts or significant changes to the implementation of the software or service.

Resources:

UPPS 03.01.05 University Income Recognition and Associated Cash-Handling Procedures

UPPS 04.01.01 Security of Texas State Information Resources

Texas State University System Policies

Texas Administrative Code 1.10.202

Payment Card Industry Security Standards Council for Merchants