To: All Account Managers and Support Staff

From: Eric Algoe
Vice President for Finance and Support Services

Date: February 14, 2018

Subj: Credit Card Acceptance

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, Information Technology, and the Information Security Office. 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 the Electronic Payment Infrastructure Team.
- 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.

If departments or individuals have any questions concerning these requirements, please contact Student Business Services at bursar@txstate.edu or call Kim Stringham at 512-245-8326 for a risk assessment.

Thank you,
Student Business Services

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