TEXAS STATE UNIVERSITY
The rising STAR of Texas

New Vendor Step-by-Step Guidance

Initial questions to ask possible Vendors:

1. Are you a TouchNet Ready Partner?
2. Can we use our own merchant account with our processor?
3. Do you have a Point-to-Point Encryption solution for card present transactions?

If the answer is no to any of these questions, be aware your request to use this vendor may be declined.

Documents required from every vendor:

1. **Attestation of Compliance for Service Provider** – This document shows they are compliant with the Payment Card Industry Data Security Standard. If they cannot or will not supply this document, we cannot do business with them.
2. **Data Flow Diagram** – This document shows how the credit card information flows through the process, network, computer, etc., from the time the card info is received, and how it is received, through the systems used to facilitate the payment, to the point of deposit.
3. **HECVAT (Cloud hosted services only) –** The Higher Education Cloud Vendor Assessment Tool is a standard tool used by all Texas schools to help us understand the details of services hosted by the Vendor. The Information Security Office will evaluate the Vendor. You can obtain the HECVAT at the following link. Be sure to complete the Service Evaluation as well. https://infosecurity.txstate.edu/services/request_service.html
4. **PA-DSS Attestation of Compliance** – Software installed on a Campus server is not preferred. Obtain the Payment Application Attestation of Compliance from the vendor. The vendor must also be listed on the PCI Council's list of validated payment applications.
5. **Point to Point Encryption Collateral** – If using PCI DSS Validated Point-to-Point Encryption hardware, obtain any collateral showing the encryption methods, the hardware, etc. P2PE hardware must also be listed as a solution on the PCI Council's website.

Step by Step

1. Ask potential vendors the three **initial questions** above. They must say YES to question #2 in order to proceed. If you want to pursue an evaluation, continue to the next step.
2. Include Information Security Office (ISO) and Electronic Payment Infrastructure Team (EPI) members in RFP process as applicable.
3. Complete the PCI Request to Use a Third Party Vendor. Obtain documents above as applicable.
4. Complete the Service Evaluation for new technology. https://infosecurity.txstate.edu/services/request_service.html. Once the evaluation is received and reviewed, you may be asked to get a completed HECVAT from the vendor if they utilize the Cloud (item 3 of "Docs required from every vendor" above).
5. Once the documents are completed, set up a meeting with the Department, the Vendor, and the Electronic Payment Infrastructure Team. Conference calls are acceptable.
6. Approval to use the Vendor must be received by **all** stake holders, including, but not limited to:
    a. Procurement and Strategic Sourcing
    b. Electronic Payment Infrastructure Team
        i. A risk assessment will be completed with decline for use OR approval with recommendations, and may require a Vice President's signature.
    c. Information Security Office
        i. Will issue decline for use OR a Data Security Plan for implementation.

7. Upon approval, obtain the contract for review by the University Legal Department. The contract must include the Texas State University System PCI DSS Addendum.
8. Begin Implementation meetings with the Vendor and TXST teams as applicable.
9. A merchant account will be set up by SBS for the solution.
10. Testing must take place to work out all nuances of the implementation.
11. Department personnel involved in using the Third Party solution must complete PCI DSS Training in SAP before going live.
12. The Department Contact for the account will work with SBS to complete all PCI Compliance documentation prior to going live.
13. Annual PCI DSS Compliance assessments will be conducted by SBS.
14. ISO and the EPI Team will review all renewals of Third Party Contracts or significant changes to the implementation of the software or service.