E-Commerce PCI DSS Compliance

Instructions: All MarketPlace users must read this document and sign below. Return completed form to k.stringham@txstate.edu

The Payment Card Industry (PCI) Data Security Standard (DSS) is made up of 12 security requirements that all entities that process, transmit, or store payment card data must comply with. As custodians of sensitive cardholder data, Texas State University uses the PCI DSS to properly secure cardholder data for all transactions, including E-Commerce transactions.

Cardholder data consists of:

- The primary account number (PAN)
- The cardholder name when associated with the PAN
- The card expiration date when associated with the PAN
- The 3 digit security code when associated with the PAN

E-Commerce Merchants must also do their part to keep cardholder data secure. E-Commerce transactions are specifically designed for the cardholders to initiate the transactions themselves from their own computers. This practically eliminates the contact that the University has with their sensitive data. As an E-Commerce merchant, you must comply with the following requirements.

- Department staff will **NOT** enter cardholder data into the TouchNet/MarketPlace application on their University computers on behalf of the cardholders. Doing so will exponentially multiply the compliance requirements which are costly and difficult.
- Departments must reconcile their E-Commerce transactions regularly to monitor the following:
  - Duplicate payments made by cardholders.
  - Attempts for fraudulent use of the Marketplace applications.
  - Payments are deposited correctly to the department's SAP accounts.
- Annual PCI awareness training must be completed and acknowledged. Signing this document will qualify as meeting this requirement.
- E-Commerce merchants that need to provide a card present form of payment for their events will contact SBS for options.

Department Name: _____ Store Name(s): _____

Printed Name	NetID	Signature	Date