

PCI Text for Agreements with Third Party Vendors

The following is language to include in agreements with Third Party Vendors involved in transmitting, processing, or storing credit card data to comply with the Payment Card Industry (PCI) Data Security Standards (DSS).

1. **Provisions For Cardholder Data.** The provisions set forth in this Section apply to third party vendors including but not limited to service providers, payment application vendors, or merchants that either themselves, through a processor, or other agent stores, processes, handles, or transmits cardholder data in any manner. For purposes of this Section, the term “cardholder data” refers to the number assigned by the card issuer that identifies the cardholder’s account or other cardholder personal information.
 - A. Third party vendors shall at all times comply with the Payment Card Industry (PCI) Data Security Standards (“PCI DSS”) requirements and is responsible for cardholder data that are prescribed in the PCI Council or the Visa Operating Regulations or otherwise issued by the PCI Council or Visa, as they may be amended from time to time (collectively, the “PCI Requirements”).
 - B. Third party vendor acknowledges and agrees that cardholder data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the PCI Council or Visa or as required by applicable law.
 - C. In the event of a breach or intrusion or otherwise unauthorized access to cardholder data stored at or for third party vendor, third party vendor shall immediately notify by fax The Ohio State University Office of the Treasurer, 614-292-7568 and by overnight mail delivered to The Office of the Treasurer at The Ohio State University, 364 W. Lane Avenue, Columbus, Ohio 43201-4340, and in the manner required in the PCI DSS Requirements, and provide the PCI Council and/or Visa and the acquiring financial institution, First Data Merchant Services, and their respective designees access to third party’s facilities and all pertinent records to conduct a review of third party’s compliance with the PCI Requirements. Third party vendor shall fully cooperate with any reviews of its facilities and records provided for in this paragraph.
 - D. Third Party vendor shall maintain appropriate business continuity procedures and systems to ensure security of cardholder data in the event of a disruption, disaster or failure of Merchant’s or third party’s primary data systems.
 - E. Third party vendor and its successors and assigns shall comply with the PCI Requirements after termination of this Agreement.

Company Name

Date

Signature

Print Name and Title