**PCI Agreement with Service Providers**

*The following is language to include in agreements with Service Providers involved in transmitting, processing, or storing credit or debit 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 service providers including but not limited to, business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. 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.

1. **<Service providers>** acknowledge in writing to the University that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the University, or to the extent that they could impact the security of the University’s cardholder data environment.
2. **<Service providers>** 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”).
3. **<Service providers>** shall detail what specific PCI requirements they manage on behalf of the merchant and what specific PCI requirements are a shared responsibility by the service provider and the university.
4. **<Service provider>** 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.
5. In the event of a breach or intrusion or otherwise unauthorized access to cardholder data stored at or for third party service provider, **<service provider>** shall immediately notify by fax The University Office of the Treasurer, 573-882-6595 and by overnight mail delivered to The Office of the Treasurer at, 118 University Hall, Columbia, MO 65211, and in the manner required in the PCI DSS Requirements, and provide the PCI Council and/or Visa and the acquiring financial institution, our merchant processor, 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 service provider shall fully cooperate with any reviews of its facilities and records provided for in this paragraph.
6. **<Service provider>** 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.
7. **<Service provider>** and its successors and assigns shall comply with the PCI Requirements after termination of this Agreement.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please Print Name Please Print Company Name