

[This Agreement must be executed substantially in the form below with any Third Party Vendor, or the following language must be substantially included in any agreement with a Third Party Vendor. NOTE: a Third Party Vendor is a service provider, other than a Merchant, that is directly involved in transmitting, processing, or storing cardholder data on behalf of OSU (as the Merchant) or provides services that control or could impact the security of cardholder data. The provisions are required in order for OSU to comply with the Payment Card Industry Data Security Standards and its agreement with its merchant processor.]

[Consider carving data breaches out of any limitation on liability provision. Most of the damages from a data breach may be classified as consequential damages. Consider requiring tech errors and omissions insurance to cover data breach damages, including consequential, vicarious and direct liabilities. Contact Risk Management to discuss.]

PCI Agreement with Third Party Vendors

This Agreement is made as of the ___ day of ____, 20__ by and between The Ohio State University (“OSU”) and _____, a _____ corporation (the “Third Party Vendor”).

For purposes of this Agreement, the following terms have the following definitions:

- (i) “cardholder data” refers to primary account number, cardholder name, expiration date and/or service code, and security-related information (including but not limited to card validation codes/values, full track data, PINs and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions;
- (ii) “cardholder data services” means services provided by Third Party Vendor to OSU that are directly involved in transmitting, processing or storing cardholder data on behalf of OSU or that control or could impact the security of cardholder data or possession of cardholder data by Third Party Vendor on behalf of OSU;
- (iii) “Merchant Account” means the account assigned to a Merchant (as defined in PCI DSS) by OSU’s acquiring bank (as defined in PCI DSS) to process cardholder payments for such Merchant;
- (iv) “Merchant Processor” means OSU’s payment card processing servicer, which is Banc of America Merchant Services, LLC as of the date hereof; and
- (v) “PCI DSS” means the Payment Card Industry (PCI) Data Security Standard requirements as then in effect.

A. PCI Acknowledgment. Third Party Vendor acknowledges to OSU that Third Party Vendor is responsible for (i) the security of cardholder data that it possesses or otherwise stores, processes or transmits on behalf of OSU, or to the extent that it could impact the security of OSU’s cardholder data environment; (ii) providing all cardholder data payment processing services for every Merchant Account for which it is processing such payments; and (iii) managing and maintaining all PCI DSS requirements. Third Party Vendor shall at all times comply with PCI DSS.

B. PCI Certification. Third Party Vendor represents and warrants to OSU that Third Party Vendor has been certified as a Level 1 service provider per PCI DSS (or any successor certification established by PCI DSS) and covenants that it will maintain such certification.

- C. Merchant Processor Registration. Third Party Vendor agrees that it or its third party online payment gateway is registered with the Merchant Processor and shall continue to remain registered with such Merchant Processor for the term of this Agreement. OSU agrees to notify Third Party Vendor of any change in its Merchant Processor.
- D. Examinations and Audits. Upon reasonable advance written notice, Third Party Vendor agrees to permit OSU (and its designees) to conduct a review of its books, records, operations and facilities during normal business hours. In addition, upon reasonable prior written notice and as directed by any card organization, Third Party Vendor agrees to permit any person acceptable to any card organization to examine and audit the records, operations and facilities of Third Party Vendor that are relevant to such card organization.
- E. Notice of Data Breach. In the event of any suspected, alleged or confirmed loss, disclosure, theft or compromise of cardholder data or card transaction information relating to the cardholder data services (a "Compromised Data Event"), Third Party Vendor shall immediately notify (i) the Office of the Chief Information Officer by leaving a voicemail at 614-688-5650 and sending an email to security@osu.edu, (ii) the Office of the Treasurer by sending a fax to 614-292-7568, and (iii) in the manner required in the PCI DSS requirements and applicable law. Third Party Vendor shall fully cooperate with any examinations provided for in the preceding paragraph. Upon Third Party Vendor's suspected or actual discovery of a Compromised Data Event, Third Party Vendor will not alter or destroy any related records and will maintain complete and accurate documentation regarding any modifications made to the records. If the systems under control of Third Party Vendor or a direct or indirect third party vendor under contract with Third Party Vendor or any additional parties under contract with the third party are at fault in connection with the Compromised Data Event, Third Party Vendor agrees to indemnify, defend and hold OSU harmless for any loss, damage or costs (including reasonable attorneys' fees) and liabilities directly or indirectly resulting therefrom (including, but not limited to, penalties, fines, notification costs, forensic investigation and remediation costs, credit card reissuance costs, credit card monitoring services and any fines, penalties and costs imposed by law or regulatory authorities). As required by Ohio law, Third Party Vendor's defense of any claim shall be subject to the Ohio Attorney General's right to appoint counsel and approve settlements.
- F. Business Continuity. 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 Third Party Vendor's primary data systems.
- G. Compliance with Applicable Law. Third Party Vendor shall comply with all applicable laws relating to cardholder data services.
- H. Term. The term of this Agreement shall commence on the date hereof and continue so long as Third Party Vendor provides cardholder data services.

[THIRD PARTY VENDOR]

THE OHIO STATE UNIVERSITY

 Name:
 Title:

 Name:
 Title: