PCI DSS Compliance Addendum

Whereas the Board of Regents of the University of Oklahoma ("University") secures services from _____ ("Vendor") under an agreement ("Agreement") dated _____ (date), which services involve the processing of merchant card transactions, specifically _____; and

Whereas University is required to adhere to the Payment Card Industry Data Security Standard (PCI DSS) promulgated by the PCI Security Standards Council; and

Whereas Vendor processes, transmits, and/or stores cardholder data ("Covered Data") in the performance of services provided to University, and is therefore considered a "service provider" under Requirement 12.8 of the PCI DSS; and

Whereas Requirement 12.8.2 of the PCI DSS requires the University to maintain a written agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data that the service provider possesses or otherwise stores, processes, or transmits on behalf of the University; and

Whereas Requirement 12.8.4 of the PCI DSS requires the University to maintain a program to monitor the service provider's PCI DSS compliance status at least annually;

It is hereby agreed that:

1) Vendor agrees that it is responsible for the security of cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data.

2) Vendor affirms that, as of the effective date of this Addendum, it has complied with all applicable requirements to be considered PCI DSS compliant, and has performed the necessary steps to validate its compliance with the PCI DSS.

3) Vendor agrees to supply the current status of Vendor's PCI DSS compliance status, and evidence of its most recent validation of compliance upon execution of this addendum to University. Vendor must supply to University a new status report and evidence of validation of compliance at least annually.

4) Vendor will immediately notify University if it learns that it is no longer PCI DSS compliant and will immediately provide University the steps being taken to remediate the non-compliance status.

5) Vendor acknowledges that it will indemnify University for any failure of Vendor to be and to remain PCI DSS compliant and for any failure of Vendor to maintain the security of cardholder data that it possesses.

6) Vendor will notify University of any breach of University data within forty-eight (48) hours of Vendor's actual or reasonable knowledge of such breach.

7) Vendor shall, upon termination, cancellation, expiration or other conclusion of the Agreement, securely destroy all instances of Covered Data in its possession. This provision shall also apply to all Covered Data that is in the possession of subcontractors or agents of Vendor. Vendor shall complete such secure destruction not more than thirty (30) days after the conclusion of this Agreement. Within such thirty (30) day period, Vendor shall certify in writing to Institution that such secure destruction has been completed. Destruction of data includes any and all copies of the data such as backup copies created at any Vendor or Vendor subcontractor site.