Service Provider Agreement Addendum

APPLICABILITY: Agencies utilizing a third-party "service provider" to process merchant cards are subject to complying with Requirement 12.8 of the PCI Data Security Standard (PCI DSS), which requires a "written agreement" addressing PCI DSS responsibilities. The requirement is one of the items included in the Self-Assessment Questionnaire (SAQ C or SAQ D) that the agency must answer annually.

Whereas Western Carolina University ("Agency") secures services from ________________ ("Vendor") under a Contract dated _____ (date), which services involve the processing of merchant card transactions, specifically ___________________________; and

Whereas Agency 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 in the performance of services provided to Agency, 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 Agency 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; and

Whereas Requirement 12.8.4 of the PCI DSS requires the Agency to maintain a program to monitor the service provider’s PCI DSS compliance status;

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 Agency. Vendor must supply to Agency a new status report and evidence of validation of compliance at least annually.

4) Vendor will immediately notify Agency if it learns that it is no longer PCI DSS compliant and will immediately provide Agency the steps being taken to remediate the non-compliance status. In no event should Vendor’s notification to Agency be later than seven (7) calendar days after Vendor learns it is no longer PCI DSS complaint.

5) Vendor shall notify and require that any Vendor sub-contractor that performs PCI DSS related service(s) pursuant to the Service Provider Agreement and this Service Provider Agreement Addendum be bound by the terms and conditions found in this Service Provider Agreement Addendum.
6) Vendor acknowledges that any indemnification provided for under the referenced Contract applies to the failure of the Vendor to be and to remain PCI DSS compliant.

(Vendor Name)

By: __________________________

Printed Name: ______________________

Title: ____________________________

Date: ____________________________

Western Carolina University

By: __________________________

Printed Name: David O. Belcher

Title: CHANCELLOR

Date: 5 November 2015

Approved as to form.

Attorney