# PCI Appendix

In addition to the terms in the ISPA, the following terms will apply if the Services provided under this Agreement involve processing credit and/or debit card transactions.

1. **Payment Card Industry Data Security Standard.** For e-commerce business and/or payment card transactions, Vendor will comply with the requirements and terms of the rules of all applicable payment card industry associations or organizations, as amended from time to time (PCI Security Standards), and be solely responsible for security and maintaining confidentiality of payment card transactions processed by means of electronic commerce up to the point of receipt of such transactions by a qualified financial institution.

2. Vendor will, at all times during the term of this Agreement, be in compliance with the then current standard for Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS) for software, and PIN Transaction Security (PCI PTS) for hardware. Vendor will provide attestation of compliance to UA annually by delivering to UA current copies of the following: (i) Vendor's "Attestation of Compliance for Onsite Assessments – Service Providers;" (ii) an attestation that all UA locations are being processed and secured in the same manner as those in Vendor's "PCI Report on Compliance;" and (iii) a copy of Vendor's PCI Report on Compliance cover letter. Vendor will notify University immediately if Entity becomes non-compliant, and of the occurrence of any security incidents (including information disclosure incidents, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities) in accordance with the ISPA.

3. Vendor's services must include the following:

   (a) Vendor maintains its own network operating on its own dedicated infrastructure. Vendor's network includes a firewall that: (i) includes access control rules that separate Vendor's PCI network from University, and (ii) restricts any communication between Vendor's network devices and University systems.

   (b) Vendor treats the University network as an untrusted network and no unencrypted cardholder data traverses or otherwise is stored on University network, and University has no ability to decrypt cardholder data.

   (c) All devices must be SRED (secure reading and exchange of data), EMV (Europay, MasterCard and VISA) and PTS POI compliant.