UNIVERSITY OF WASHINGTON

PCI COMPLIANCE RIDER

INTRODUCTION, PARTIES, AND EFFECTIVE DATE

THESE **PCI COMPLIANCE** TERMS HEREBY INCORPORATED INTO THE CONTRACT BETWEEN THE UNIVERSITY OF WASHINGTON (UNIVERSITY) AND CONTRACTOR, AS OF THE "EFFECTIVE DATE" OF THE CONTRACT. IN CONSIDERATION OF THE MUTUAL PROMISES IN THE CONTRACT AND OTHER GOOD AND VALUABLE CONSIDERATION, THE PARTIES AGREE AS FOLLOWS:

I. DEFINITIONS

1. "**PCI DSS**" is the Payment Card Industry (PCI) Data Security Standard (DSS).
2. **"Cardholder Data"** as defined by the PCI DSS consists of the full primary account number and any of the following associated with it: cardholder name, expiration data and the service code.
3. "**SERVICE PROVIDER"** as used herein this PCI Compliance Rider refers to the meaning defined within the latest version of PCI DSS.

II. DECLARATIONS

Parties understand and acknowledge:

1. Contractor is a Service Provider.
2. Contractor is responsible for the security of all cardholder data in Contractor's possession.
3. Contractor may only use cardholder data completing the contracted services as described in this Contract, or as required by the PCI DSS, or as required by applicable law.
4. All items in this rider apply to any and all subcontractors utilized by the Contractor.

III. SERVICE PROVIDER RESPONSIBILITY

1. STANDARD OF CARE
    a. Contractor has implemented and shall maintain safeguards against the destruction, loss or alteration of payment card information that is in the Contractor's possession or under Contractor's care unless prescribed by PCI DSS.
    b. Contractor warrants that its operations with respect to the security for cardholder data shall be performed in accordance with industry best practices by qualified personnel, and further evidenced through compliance with PCI DSS, as specified in the following provision.

2. COMPLIANCE WITH PCI DSS

   a. Contractor represents and warrants that for the life of the contract and/or while Contractor has possession of University customer cardholder data, devices, software and services used for storage, processing, or transmitting transactions shall be compliant with standards established by the Payment Card Industry (PCI) Security Standards Council (https://www.pcisecuritystandards.org)

   b. Contractor shall, at its own expense, obtain an Attestation of Compliance from a Qualified Security Assessor (QSA) as defined by the standards established by the Payment Card Industry (PCI) Security Standards Council.

   c. Upon written request, Contractor shall furnish University with an Attestation of Compliance with the Payment Card Industry Data Security Standard (PCI DSS) within 10 business days of the date of the request.

   d. In instances where the University permits the Contractor to utilize University network connectivity to the Internet, Contractor acknowledges and agrees that the University is acting in the role of an Internet Service Provider in offering only unmanaged connectivity. University does not warrant the security and suitability of such connectivity for payment processing and related communications. Contractor assumes all risk and responsibility related to any such use of University Internet connectivity.

   e. In instances where the Contractor serves as Merchant of Record, the Contractor shall assume all risk, responsibility, and liability for protecting payment card data it processes on behalf of the University's customers.

   f. In instances where the University is serving as merchant of record, any payment card terminals provided or sold from the Contractor must be certified Point to Point Encrypted (P2PE) with chip and tap technology.

3. REMEDIATION AND INCIDENT MANAGEMENT

   a. In the event of a finding by QSA, or some other circumstance whose consequence is that Contractor is not actually in compliance with PCI DSS, then Contractor shall:

      i. Immediately inform the University of the nature of the PCI DSS compliance deficiencies.

      ii. Promptly plan such remedial actions as necessary to cure any and all PCI DSS compliance deficiencies. Within 30 days, the Contractor shall review their remediation plan with a QSA and obtain a written confirmation of the QSA's opinion that such plan will remediate Contractor's PCI DSS deficiencies. Contractor shall then promptly execute this QSA-reviewed remediation plan.

   b. In the event of a data breach or intrusion or otherwise unauthorized access to cardholder data for which Contractor is responsible, Contractor shall notify University's

Office of Merchant Services no later than 48 hours of confirming the Data Breach to allow the proper PCI DSS compliant breach notification process to commence.

4. CREDIT CARD INFORMATION INDEMNIFICATION

   a. It is the intent of the parties that all indemnity obligations of Contractor with respect to **PCI Compliance** be allocated within this section, notwithstanding any exclusion or limitation of liability language elsewhere within this Contract. The Contract shall be interpreted accordingly.

   b. Contractor agrees to defend, indemnify and hold harmless, the University, its officers, employees, and agents, from and against any and all claims, demands, causes of action, suits, proceedings, judgment, award, damages, costs (including reasonable attorneys' fees), expenses, fees, losses, fines of a penal nature, civil penalties, and other liabilities (including the obligation to indemnify others) arising from or connected to any loss of University customer credit card or identity information managed, retained or maintained by Contractor, including but not limited to fraudulent or unapproved use of such credit card or identity information.

5. INSURANCE COVERAGE

The indemnities within these PCI compliance terms shall be supported by appropriate types and amounts of insurance, as further specified in the IT Security Terms Rider hereby incorporated by reference.