Data Security Addendum

As used in this Data Security Addendum, the term "WSU" shall mean Washington State University and the term "Supplier" shall mean the counterparty to the applicable agreement, purchase order, or other contractual document between WSU and Supplier (the "Agreement"). This Data Security Addendum is expressly incorporated into the Agreement by reference. In the event of a conflict between the terms of this Data Security Addendum and the Agreement, the terms of this Data Security Addendum shall control.

a) Confidential Information

In performance of the Agreement, the parties may directly or indirectly disclose confidential information, proprietary information, or confidential data ("Confidential Information"). The party receiving information is generically referred to as the "Receiving Party," and the party disclosing the information is generically referred to as the "Disclosing Party."

"Confidential Information" shall include any data and/or information that is identified by either party as confidential (either orally or in writing) or is of such a nature that a reasonable person would understand such information to be confidential, including, but not limited to: (1) personal information of customers, employees, students, and/or donors, including but not limited to, images, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical information or data, law enforcement records, educational records or other information identifiable to a specific individual that relates to any of these types of information ("Personal Information"); (2) business methods, plans, and practices, financial data, or customers lists; (3) trade secrets, inventions, methodologies, research plans, products, product plans, patent applications, and other proprietary rights, and any specifications, tools, computer programs, source code, object code, documentation, or technical information; or (4) any other proprietary information or data the Disclosing Party maintains in confidence.

Confidential Information shall not include information the Receiving Party can prove by clear and convincing written contemporaneous evidence is: (1) publicly known through no fault or negligence of the Receiving Party; (2) rightfully possessed by the Receiving Party prior to disclosure by the Disclosing Party; (3) rightfully obtained by the Receiving Party from a third party in lawful possession of such Confidential Information without the obligation of confidentiality; (4) independently developed by the Receiving Party without reference to or use of Confidential Information; (5) required to be disclosed by law; or (6) necessary to disclose to prevent severe physical injury to or loss of life of an individual.

b) Use and Non-Disclosure of Confidential Information; Exceptions

Each party agrees to use the Confidential Information received from the other party only as expressly permitted in the Agreement or when reasonably necessary to perform the party's duties under the Agreement so long as such disclosure is in accordance with applicable law. To the extent permitted by law, neither party will disclose to any third party the other party's Confidential Information, in whole or in part, without the prior written consent of the party, or as

provided for in the Agreement and in compliance with all applicable state and federal laws. However, Supplier may disclose Personal Information of WSU students to a third party with the written consent of that student. Notwithstanding the foregoing, either party may disclose the Confidential Information or portions thereof to their respective attorneys or accountants when seeking legal or financial advice.

Supplier specifically warrants and represents that except as otherwise permitted herein, it will not in any manner disclose, disseminate, copy, sell, resell, sublicense, transmit, assign, or otherwise make available any of WSU's Confidential Information to any third party without the prior written permission of WSU. Supplier further warrants and represents that it will take all reasonable steps necessary to ensure that its authorized agents, employees, contractors or subcontractors having access to the Confidential Information shall not copy, disclose or transmit any of the Confidential Information, or any portion thereof, in any form, to a third party except as necessary to perform the Services under the Agreement.

Supplier acknowledges that WSU, as a state agency, is at all times subject to the Washington Public Records Act, RCW 42.56.010 *et. seq*. as now existing or as amended. If WSU receives a public records request for the Agreement and/or for documents and/or materials provided to WSU under the Agreement, generally such information will be a public record and must be disclosed to the public records requester. However, WSU agrees to notify Supplier if it receives such a public records request and the date WSU plans to release the records. If Supplier fails to obtain a protective order from the applicable court prior to the time WSU releases the records to the public records requester, Supplier gives WSU full authority to release the records on the date specified, and Supplier understands it shall hold WSU harmless with respect to such disclosure.

c) Obligations to Secure Confidential Information

Supplier warrants and represents that it will implement the necessary industry-standard physical, administrative, and technical safeguards to ensure the confidentiality, integrity, and availability of WSU Confidential Information, including but not limited to, the environment in which the WSU Confidential Information is stored, processed, and transmitted. Supplier further warrants and represents that such safeguards will in no event be less than the level of security Supplier uses to protect its own Confidential Information so long as it is consistent with all legal requirements for safeguarding this particular data. Supplier shall require its contractors and subcontractors authorized to access or receive WSU's Confidential Information pursuant to the Agreement to implement consistent controls and interventions to safeguard WSU's Confidential Information.

Supplier agrees to comply with all applicable state and federal statutes and regulations governing use, access and disclosure of the Confidential Information including, but not limited to: (1) personally identifiable information from education records as defined in The Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99), and regulations promulgated thereunder; (2) information that is subject to the security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C., Subchapter 1, Sections 6801-6809 (Disclosure of Nonpublic Personal Information); (3) individually identifiable health information or protected health information as defined in the Health Insurance Portability and Accountability Act of 1996

("HIPAA") regulations, 45 CFR Parts 160 and 164; (4) the Washington Uniform Health Care Information Act, RCW 70.02; and (5) the applicable Washington Technology Solutions policies (https://watech.wa.gov/policies) or comparable standard(s).

Any transmission, storage, or transportation of WSU Confidential Information outside of the U.S.A. is prohibited without prior written authorization from the WSU.

Prior to execution of the Agreement and once per calendar year, Supplier will provide WSU with the most current SSAE 18 (SOC 1 Type 2 and SOC 2 Type 2) reports, the Higher Education Community Supplier Toolkit (HECVAT), and/or comparable industry appropriate 3rd party information security assessment report. WSU shall have the right, at its own expense and upon reasonable prior notice to Supplier, to review Supplier's security controls and information security program.

If Supplier will accept and process payment by credit cards or any other form of electronic payment on behalf of WSU pursuant to the Agreement, Supplier agrees to provide evidence of certification for the Payment Card Industries Data Security Standard ("PCI DSS"). Proof of compliance shall be provided to WSU by Supplier on an annual basis for the duration of the Agreement. WSU reserves the right to monitor, audit or investigate said certification. Supplier will immediately notify WSU if Supplier fails to achieve or maintain PCI DSS compliant status. Supplier will also stop accepting and processing of payment cards or any other form of electronic payment on behalf of WSU and is prohibited from accepting any other WSU Confidential Information.

d) Obligations upon Breach of Security

The Confidential Information, including any Personal Information, is subject to the provisions of Washington's breach notification laws including RCW 19.255.010 and RCW 42.56.590. Supplier represents and warrants it will comply with these laws. Supplier will immediately report to the WSU Chief Information Security Officer (ciso@wsu.edu; 509-335-1642) and/or Chief Information Officer (cio@wsu.edu; 509-335-5016) any breach of security resulting in the unauthorized disclosure, misappropriation or unauthorized use or access of WSU Confidential Information ("Breach"). Supplier will promptly investigate any Breach affecting WSU Confidential Information in accordance with the law, and will make commercially reasonable measures to identify the Breach's root cause(s), mitigate further harm and loss, and promptly recovery from any negative impact on WSU, and prevent a recurrence. Unless prohibited by law, Supplier will provide WSU with a detailed description of the Breach, the type of data that was the subject of the incident, the identity of each affected person, and other information WSU may reasonably request concerning the affected persons. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices to the affected persons. If a Breach, or data compromise or loss occurs and is found to be the result of Supplier's non-compliance with its obligations to secure WSU Confidential Information, Supplier will assume complete responsibility for customer notification, and be liable for all associated costs and professional fees incurred by WSU in responding to or recovering from that Breach or loss.

e) Survival of Obligations

The obligation to maintain the confidentiality of the Confidential Information received by the other party will survive termination or expiration of the Agreement, and to the greatest extent permitted by law shall survive for as long as the other party maintains that information. Except as otherwise set forth below, within sixty (60) days of the expiration or termination of the Agreement, Supplier shall, at Supplier's option: (1) certify in writing to WSU that Supplier has destroyed all WSU Confidential Information in its possession; or (2) return all media containing all WSU Confidential Information to WSU and certify in writing the return of such Confidential Information; or (3) take whatever other steps WSU requires of Supplier to protect WSU's Confidential Information. WSU reserves the right to audit, or investigate the use of WSU Confidential Information collected, used, or acquired by Supplier or its employees, contractors or subcontractors pursuant to the Agreement. Any costs of such audit or investigation are the sole responsibility of WSU.