Data Security Addendum

Contractor acknowledges that the Contract between the Parties allows the Contractor access to Covered Data and Information ("CDI"), as defined below. This Data Security Addendum adds additional obligations concerning the use of CDI to the Contract between the parties.

1. Definitions

a. The following words or phrases, as used in this Section, shall be given the same definition as they are given in the Pennsylvania Breach of Personal Information Notification Act, 73 P.S. § 2301 et seq., as may be amended: "**Breach of the security of the system**," "**Determination**," "**Discovery**," and "**Personal Information**."

b. **Covered Data and Information ("CDI")** - includes (1) paper and electronic financial information that is marked as confidential; (2) Personal Information; (3) personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act ("FERPA"), 20 USC 1232g; (4) "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act ("HIPAA"), 45 CFR Part 160.103; (5) nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999 ("GLB"), 15 USC 6809; (6) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; (7) other financial account numbers, access codes, driver's license numbers; state- or federal-identification numbers such as passport, visa or state identity card numbers; (8) and any other data marked as non-public that is provided by the University, its students or a third party to the Contractor to perform the services under this Contract.

c. **Covered Parties** - The following are considered a "Covered Party" subject to the restrictions on the use of CDI: Contractor; employees or agents of Contractor who actually and legitimately need to access or use CDI in the performance of Contractor's duties to University; and such third parties, such as but not limited to subcontractors, who have an actual and legitimate need to access or use CDI.

d. **System** - An assembly of components that supports an operational role or accomplishes a specific objective including a discrete set of information resources (network, server, computer, software, application, operating system or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

e. **Notice** - In addition to all other Notice requirements provided for pursuant to any agreement into which this Data Security Addendum is incorporated, any notice required of Contractor pursuant to this Data Security Addendum shall be made by email directed to: ContractorCyberIncident@passhe.edu.

2. Use of, Disclosure of, Storage of, or Access to CDI

a. Contractor and Covered Parties shall only use, disclose, store, or access CDI In accordance with, and only to the extent permissible or necessary to fulfill obligations under the Contract, this Addendum and any other agreement between the parties and will not share CDI with or disclose it to any third party without the prior written consent of the University, except as required by the Contract or as otherwise required by applicable law.

b. Contractor and Covered Parties shall only use, disclose, store, or access CDI in full compliance with any and all applicable laws and regulations, only to the extent applicable to Contractor, including but not limited to: FERPA, HIPAA, GLB, Federal Trade Commission Red Flags Rule, the Social Security Act, Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), U.S. export control laws, the European Union General Data Protection Regulation (GDPR), and personnel and data breach laws of the Commonwealth of Pennsylvania.

c. Contractor will ensure all internal Covered Parties have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of the Contract and this Addendum.

d. Contractor shall require all third party Covered Parties to agree in writing and in advance of any disclosure, to be bound by confidentiality terms at least as stringent as the terms of this Addendum.

e. Any transmission, transportation, or storage of CDI outside the United States is prohibited except on prior written authorization by the University.

f. Contractor and Covered Parties may store CDI on servers housed in datacenters owned and operated by third parties, provided the third parties have executed confidentiality agreements with Contractor that are consistent with the Contract and this Addendum.

g. For CDI subject to FERPA, Contractor will be considered a "school official" with a "legitimate educational interest" as those terms are used in FERPA and its implementing regulations. Contractor agrees to abide by the limitations and requirements imposed on school officials. Contractor will use the education records only for the purpose of fulfilling its duties under the Contract for University's and its end user's benefit and will not share such data with or disclose it to any third party except as provided for in the Contract, required by law, or authorized in writing by the University.

h. The parties agree that as between them, all rights including all intellectual property rights in and to CDI shall remain the exclusive property of the University, and Contractor has a limited, nonexclusive license to use the data as provided in the Contract solely for the purpose of performing its obligations under the Contract. The Contract does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Contract.

3. Safeguarding CDI

a. Contractor shall ensure that its employees have undergone appropriate background screening and possess all needed qualifications to comply with the terms of the Contract and this Addendum, including but not limited to all terms relating to data and intellectual property protection.

b. Contractor agrees that use, storage, and access to CDI shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices designed and implemented in such a manner to ensure the confidentiality, availability, and integrity of CDI and to avoid or prevent compromises, attacks and potential Data Breaches.

c. Contractor will implement the controls reasonably necessary to protect any System owned or operated by Contractor that contains CDI: (1) using secure protocols and encryption to safeguard CDI in transit; (2) adding a host-based or external firewall to protect the System (or allowing the University to add a host-based or external firewall); (3) limiting administrative and remote access to the System; (4) limiting account access and privileges to the least necessary for the proper functioning of the System; (5) removing or disabling applications and services that are not necessary for the proper functioning of the System; (6) utilizing named user accounts and not generic or shared accounts; (7) utilizing Federated Single Sign On, Kerberos, or other industry compliant services for authentication and authorization; (8) avoidance of default passwords and capabilities that allow the changing of System and user passwords; (9) enabling an appropriate level of auditing and logging for the operating system and applications; and (10) take reasonable measures to protect CDI against deterioration or degradation of data quality and authenticity.

d. The University reserves the right to request security information reasonably necessary to ascertain University's own compliance with state and federal data privacy laws. Upon the University's request, Contractor shall provide a copy of its most recent SOC 2 report, and that of any data center in which CDI is stored. The University may also require the Contractor to complete a Higher

Education Cloud Vendor Assessment Tool (HECVAT) to ensure the services to be provided are appropriately assessed for security and privacy needs. Contractor agrees to cooperate with the University to ensure data is handled and systems are operated in compliance with applicable University policy and adopted standards.

e. If the Contractor maintains or stores computerized data on behalf of the University that constitutes Personal Information the Contractor shall:

   i. Utilize encryption, or other appropriate security measures, to reasonably protect the transmission of personal information from being viewed or modified by an unauthorized third party. The Contractor shall develop and maintain (or continue to maintain if such a policy already exists) a policy to govern the proper encryption or other appropriate security measures and transmission of data to the University. In developing the policy, the Contractor shall reasonably consider similar existing Federal policies and other policies, best practices identified by other states and relevant studies and other sources as appropriate in accordance with best practices as established by the Federal Government and the Commonwealth of Pennsylvania. The policy shall be reviewed at least annually and updated as necessary.

   ii. Develop (or continue to maintain if such a policy already exists) a policy to govern reasonably proper storage of the Personal Information. A goal of the policy shall be to reduce the risk of future breaches of the security of the system. In developing the policy, the Contractor shall reasonably consider similar existing Federal policies and other policies, best practices identified by other states and relevant studies and other sources as appropriate in accordance with best practices as established by the Federal Government and the Commonwealth of Pennsylvania. The policy shall be reviewed at least annually and updated as necessary.

4. Product Maintenance and Support

a. Contractor shall have a process for the timely review, testing, and installation of patches essential for safeguarding the confidentiality, integrity, or availability of the System or CDI.

b. Contractor will implement best practices for change management procedures, including a formal process to ensure that changes to a System are introduced in a controlled and coordinated manner to avoid or reduce the possibility that unnecessary changes, faults or vulnerabilities are introduced to the System, or that changes made by other users are undone.

c. Contractor shall ensure that all products under subscription are remotely supported via a secure connection method that includes an audit log of events. Remote access shall be limited to an as needed or as requested basis. Contractor shall provide University with notice 12 months before the product becomes unsupported.

5. Contractor Access to University Systems

a. In accordance with applicable policies, University login credentials may be given to contractors for the purposes of scheduled troubleshooting, maintenance, or updates to software provided or supplied by Contractor and installed on University-owned computer equipment. In such a case, the University will provide the Contractor with credentials for logging in locally or through a secured Virtual Private Network (VPN), if required. Credentials will be issued by the University through a help desk ticket and issued for a specified time and disabled once that time has expired.

b. As a condition of the Contractor's access to University computing equipment the Contractor represents that they will not attempt to access any system(s) other than the one(s) designated in the help desk ticket.

c. All work performed by the Contractor while connected to University computing equipment may be monitored or verified by the University.

6. Data or Security Incident

a. Upon Contractor's Discovery that a Breach of the security of the system has occurred, or that CDI may otherwise have been accessed, disclosed, or acquired without proper authorization, Contractor shall immediately, and in no event more than 24-hours following Determination of the Breach of the security of the system, provide Notice to the University. Contractor shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the incident. Contractor shall give highest priority to immediately correcting any incident and shall devote such resources as may be required to accomplish that goal. Contractor shall fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident.

b. Contractor shall promptly provide the University information necessary to enable the University to fully understand the nature and scope of the incident so that it can take appropriate action, including notice to individuals impacted and, if need be, notice to consumer reporting agencies as required by the Commonwealth's Breach of Personal Information Notification Act, 73 P.S. §§ 2301 et seq.

c. In addition to any other remedies available to the University under law or equity, Contractor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any incident, including but not limited to providing notification to individuals whose CDI was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the CDI exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the incident.

d. Upon request, Contractor shall provide University information about what Contractor has done or plans to do to mitigate any deleterious effect of the unauthorized use or disclosure of, or access to CDI. In the event that an incident requires Contractor's assistance in reinstalling software, such assistance shall be provided at no cost to the University. The University may discontinue any services or products provided by Contractor until the University, in its sole discretion, determines that the cause of the incident has been sufficiently mitigated.

e. The Contractor shall coordinate all outbound communications regarding an incident with the University.

f. Notification following Breach of the Security of the System: Upon Determination that a Breach of the security of the system has occurred, Contractor shall, in addition to the above requirement regarding notification of the State System, comply with all relevant state and federal laws and regulations regarding notification of data breach, including, but not limited to, the Pennsylvania Breach of Personal Information and Notification Act, 71 Pa.C.S. § 2031, *et. seq*.

7. Compelled Disclosure of CDI

a. Contractor shall promptly notify the University in writing of any subpoena, discovery request, court order, or other legal request or command to disclose CDI and provide the University sufficient time to obtain a court order or take any other action the University deems necessary to prevent disclosure or otherwise protect CDI. Contractor shall provide prompt and full cooperation in University's efforts to protect CDI. Upon request, Contractor will provide the University with a copy of its response.

b. If the University receives a subpoena, discovery request, court order, or other legal request or command (including a request pursuant to the Pennsylvania Right to Know Law) or request seeking CDI maintained by Contractor, the University will promptly provide a copy to Contractor. Contractor will promptly supply the University with copies of data required for the University to respond and will cooperate with the University's reasonable requests in connection with its response.

8. Data Transfer or Destruction Procedures

a. Upon expiration or termination of the Contract, Contractor shall follow the University's instructions as to the preservation, transfer, or destruction of CDI. Any transfer to the University or a designated third party shall occur within a reasonable period of time and without significant interruption in service. Contractor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to CDI during the transition.

b. In the event the University requests destruction of CDI, Contractor agrees to destroy all data in its possession and in the possession of any subcontractors or agents to which the Contractor might have transferred CDI in accordance with standards that meet or exceed National Institute of Standards and Technology (NIST) Special Publication 800-88r1 guidelines pertaining to data sanitization using "purge" or "destroy" methods. Contractor agrees to provide documentation of data destruction.

c. Contractor will notify the University of an impending cessation of its business and any contingency plans, immediately transfer any previously escrowed assets and CDI and provide the University access to facilities to remove and destroy University-owned assets and CDI. Contractor shall take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. Contractor will also provide a full inventory and configuration of all hardware and software involved in service delivery. Contractor will work closely with its successor to ensure a successful transition in advance of the final transition date, with minimal downtime and effect on the University. Upon request by the University, Contractor shall certify in writing to University that return or destruction of data has been completed. Prior to such return or destruction, Contractor shall continue to protect CDI in accordance with the terms of the Contract and this Addendum.

d. The Contractor's obligations under this section shall survive termination of the Contract until all CDI has been returned or securely destroyed.