Data Protection Addendum

This Data Protection Addendum ("Addendum") is an add-on to, and incorporated as part of:

☐the Montgomery College ("College") Purchasing Terms and Conditions at https://info.montgomerycollege.edu/_documents/offices/procurement/docs/purchase-order-terms-and-conditions.pdf, applicable in those situations where the Selected Firm/Vendor ("Vendor") provides goods or services under a Purchase Order ("Agreement") pursuant to which the Vendor creates, obtains, transmits, receives, uses, maintains, processes, stores, or disposes of College Data (defined within).

☐ An agreement of even date herewith between Montgomery College ("College") and _____ ("Vendor") (hereinafter, "Agreement") pursuant to which Vendor provides services and or solutions and Vendor creates, obtains, transmits, receives, uses, maintains, processes, stores, or disposes of College Data (defined within).

This Addendum sets forth the terms and conditions pursuant to which College Data will be protected by Vendor during the term of the Parties' Agreement and after its termination.

A. Acknowledgement of Confidential Nature of Information, Access and Applicable Law

Vendor acknowledges that its performance of Services under the License Agreement may involve access to confidential data of the College as contemplated in College Policy and Procedure 66002 including, but not limited to, personally-identifiable information, student records and information, protected health information, or individual financial information (collectively, "Protected Information"). Protected information may be subject to state, federal and/or international laws/rules restricting the use and disclosure of such information, (collectively, "Data Protection Laws") including, but not limited to:

1. Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2));
2. Federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) and 34 CFR Part 99;
3. Health Insurance Portability and Accountability Act and its implementing regulations (including without limitation 45 CFR Part 160 and Subparts A, C, and E of Part 164);
4. Payment Card Industry Data Security Standards promulgated by the PCI Security Standards Council;
5. Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation), (collectively, "GDPR");
6. Maryland Protection of Personally Identifiable Information by Public Institutions of Higher Education, MD State Gov't. §§10-13A-01 *et seq.*;
7. MD State Gov't. Article, §10-1305; and
8. Such other federal, state and local laws and regulations and College policies governing the proper storage, handling, use, sharing, transmission and possessing of Protected Information.

Vendor shall comply with, and require subcontractors to comply with, all Data Protection Laws applicable to Protected Information and Vendor's storage, handling, use, sharing, transmission and possessing of Protected Information. Vendor agrees that it maintains a privacy governance program that conforms to the Data Protection Laws.

B. Prohibition on Unauthorized Use or Disclosure of Protected Information

Vendor agrees to hold Protected Information, and any information derived from such Protected Information, in strictest confidence. Vendor shall not access, use or disclose Protected Information except

as permitted or required by the Agreement or as otherwise authorized in writing by the College, Data Protection Laws, or other applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected Information, Vendor will notify College in writing within one business day upon receiving notice of such requirement and prior to any such disclosure, to give College an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). If such opposition is unsuccessful, or if the College does not otherwise oppose or respond to the disclosure notice, Vendor shall provide to the College a copy of any Protected Information disclosed contemporaneously with its disclosure. Any transmission, transportation or storage of Protected Information outside the United States is prohibited except on prior written authorization by the College.

Notwithstanding any other provisions of this Agreement, this Section B does not prohibit or limit Vendor from any use or disclosure of any information that may be the same as any Protected Information which Vendor can demonstrate by documentary evidence was (i) properly obtained by Vendor outside of its Agreement with the College and without access to, reference to or use of any Protected Information, and (ii) at all times maintained separately from and not in any way combined, commingled, compared, benchmarked or in any way associated with any Protected Information.

C. Safeguard Standard

With respect to the College's Protected Information, Vendor shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the College's Protected Information, and that are reasonably designed to protect the Protected Information from unauthorized access, use, modification, disclosure or destruction.

If Vendor discovers a breach of its security system, Vendor shall notify the College as stated herein and in accordance with the requirements of MD State Gov't. Article, §10-1305, or successor provision and shall comply in all respects reasonably pertinent to the Agreement with requirements of Data Protection Laws.

Vendor agrees to protect the privacy and security of Protected Information according to all Data Protection Laws and regulations, by industry standard & commercially-acceptable standards, and no less rigorously than it protects its own confidential information. Vendor has reviewed College's Policy and Procedure 66002 and supports the privacy governance program of the College as reflected therein and in other documentation provided by College in connection with entering into the Agreement. Vendor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality (authorized access), integrity and availability of the Protected Information. While Vendor has responsibility for the Protected Information under the terms of this Addendum, Vendor shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities.

1. All facilities used to store and process Protected Information will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

2. Vendor components must employ TLS 1.2 or greater for all College data in-transit including any website or application portal. All data at rest must be encrypted using at least the industry standard encryption algorithm AES-128 or greater.

3. Vendor warrants that the Vendor products and/or services (including any products and/or services provided by affiliates or subcontractors) must support federated single sign-on (SSO) using SAML 2.0 or Active Directory Federation Services 4.0 and higher to allow College users to leverage Montgomery College credentials and enforce its authentication policies, including multi-factor authentication.

4. Vendor will require its employees and those of its affiliates and subcontractors to use multi-factor authentication to connect to all partner and sub-contractor systems that handle College data (at rest or in transit).

5. Vendor will use industry standard and up-to-date security tools and technologies such as antivirus protections and intrusion detection methods in providing Services under the Agreement.

6. Vendor shall store or process Protected Information only in data centers located in the United States unless the College agrees in writing to another location.

7. Vendor must provide role-based access control to ensure that only authorized individuals are granted access to the offered solution with permissions granted appropriate to their role.

8. Vendor will provide certification from 3rd party auditor of latest SOC 2 Type 2 audit, upon request by Montgomery College.

D. Artificial Intelligence Use and Data Protection

If Vendor uses Artificial Intelligence ("AI") or Machine Learning ("ML") technologies in providing products or services under this Agreement, Vendor shall:

1. **Prohibit AI Training on Protected Information**
   Vendor shall not use College Protected Information, or any derivative thereof, for training, fine-tuning, or improving AI/ML models.

2. **Ensure Compliance with Data Protection Laws**
   Any AI/ML processing of Protected Information must comply with all applicable Data Protection Laws and College policies, including GDPR, FERPA, HIPAA, and Maryland statutes.

3. **Maintain Transparency and Explainability**
   Vendor shall disclose to the College any AI/ML components that process Protected Information and provide documentation describing how such components operate, including data flow diagrams and risk assessments.

4. **Implement Technical and Organizational Safeguards**
   Vendor shall ensure AI/ML systems incorporate privacy-by-design principles, including:
   - Data minimization and purpose limitation.
   - Encryption of data in transit and at rest.
   - Role-based access controls for AI outputs.

5. **Prevent Unauthorized Retention or Re-identification**
   Vendor shall implement measures to prevent AI systems from retaining Protected Information beyond the processing purpose or performing re-identification of anonymized data.

6. **Audit and Monitoring Rights**
   College reserves the right to audit AI/ML systems handling Protected Information to verify compliance with this Addendum and applicable laws.

E. Return and Destruction of Protected Information

Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, Vendor shall return the Protected Information to College in an agreed upon format, and Vendor must destroy any copies of Protected Information remaining within its possession or control. This provision shall also apply to all Protected Information that is in the possession or control of affiliates or subcontractors of Vendor. Such destruction shall be accomplished by "purging" or "physical destruction" in accordance with commercially reasonably standards for the type of data being destroyed (e.g., Guidelines for Media Sanitization, NIST SP 800-88). Vendor shall certify in writing to College that such return and destruction has been completed. Vendor's affiliates and subcontractors must also make such certification to College.

F. Breaches of Protected Information

For purposes of this section, the term "Breach," has the meaning given to it under the Data Protection Laws and/or regulation.

1. Reporting of Breach. Within one business day upon discovery of a confirmed Breach, Vendor shall report in writing to the College. In the event of a suspected Breach, Vendor shall keep the College informed regularly of the progress of its investigation until the uncertainty is resolved.

Vendor's report shall identify:

a) The nature of the unauthorized access, use or disclosure,

b) The Protected Information accessed, used or disclosed,

c) The person(s) who accessed, used and disclosed and/or received Protected or Private Information (if known),

d) What Vendor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and

e) What corrective action Vendor has taken or will take to prevent future unauthorized access, use or disclosure.

f) Vendor shall provide such other information, including a written report, as reasonably requested by College.

2. Coordination of Breach Response Activities.

In the event of a confirmed Breach, Vendor will:

a) Immediately preserve any potential forensic evidence relating to the Breach;

b) Promptly (within 2 business days) designate a contact person to whom the College will direct inquiries, and who will communicate Vendor responses to College inquiries;

c) As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore College service(s) as directed by the College, and undertake appropriate response activities;

d) Provide status reports to the College on Breach response activities, either on a daily basis or a frequency approved by the College;

e) Coordinate all media, law enforcement, or other Breach notifications with the College in advance of such notification(s), unless expressly prohibited by law;

f) Make all reasonable efforts to assist and cooperate with the College in its Breach response efforts; and

g) Ensure that knowledgeable Vendor staff are available on short notice, if needed, to participate in College-initiated meetings and/or conference calls regarding the Breach.

3. PCI Compliance. College is required to maintain a program to monitor a third-party service provider's PCI DSS compliance at least annually. If Vendor is responsible as a "service provider" under Requirement 12.8 of the PCI DSS for the security of cardholder data that it possesses, or that passes through it relating to receiving, storing, processing, and transmitting of the cardholder data, it must at all times comply with all applicable requirements of, and annually validate such compliance with, the PCI DSS. Vendor will annually provide the College with evidence of its current validation of compliance with PCI DSS requirements. Such evidence must be specific and sufficient to enable the College to confirm that all applicable PCI DSS requirements are met. Vendor shall immediately notify College if it learns that it is no longer PCI DSS compliant and will immediately provide the College with the steps being taken to remediate the non-compliance status. Vendor is responsible to ensure that its affiliates and/or subcontractors comply with this provision.

4. Costs Arising from Breach. In the event of a Breach (including of payment card data) by the Vendor (or its employees, officers, directors, subsidiaries, and agents, Vendor agrees, up to the greater of the coverage of the limitation of liability in the Underlying Agreement, or the insurance coverage below, to promptly reimburse all costs to the College arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of College personnel responding to Breach, civil or criminal penalties levied against the College, attorney's fees, court costs, etc. Any such Breach may be grounds for immediate termination of the Agreement by the College.

G. Examination of Records

Subject to applicable law and upon reasonable written request, College shall have access to and the right to examine any pertinent books, documents, papers, and records of Vendor involving transactions and work related to the Agreement and this Addendum until the expiration of three years after final payment hereunder. Vendor shall retain project records for a period of three years from the date of final payment**.**

H. Assistance in Litigation or Administrative Proceedings

Vendor shall make itself and any employees, subcontractors, or agents assisting Vendor in the performance of its obligations under the Agreement and Addendum available to College at no cost to College to testify as witnesses in the event of an unauthorized disclosure caused by Vendor that results in litigation or administrative proceedings against College, its directors, officers, agents or employees based upon a claimed violation of laws relating to security, privacy or arising out of this agreement.

I. Insurance

Vendor shall maintain at all times during the term of the Agreement, at its own expense, cyber liability and technology errors and omissions insurance as specified below.

All policies of insurance will be issued by insurers authorized to transact business in the State of Maryland and authorized to issue policies of insurance. Vendor will deliver certificates of insurance evidencing the required insurance coverages to College within five (5) business days following the Execution Date of this Fourth Amendment. Each of these insurance policies shall be issued by insurance companies each with an AM Best Rating of "A-" or its functional equivalent:

Insurance Policy	Minimum Coverage
Workers Compensation	As required by state law
Professional Liability (including Cyber Liability)	$2,000,000 per occurrence/aggregate
Commercial General Liability	$1,000,000 per occurrence $2,000,000 aggregate
Comprehensive Automobile Liability	$1,000,000 combined single limit – bodily injury and property damage

If the above insurance coverage is cancelled and not replaced with other coverage meeting the above requirements, Vendor will provide College with not less than thirty (30) days advance written notice of such cancellation, and will promptly obtain replacement coverage that complies with this Section

J. Conflict

In the event of any conflict between this Addendum and any click-wrap, posted provisions, or other provision in Vendor documents, the provisions of this Addendum shall control.

K. Survival

The Vendor shall maintain an industry standard disaster recovery program to reduce in potential effect of outages because of supporting data center outages. Any backup site used to store College Protected Information shall include the same information security and privacy controls as the primary data center(s).

This Data Protection Addendum is agreed to and entered into by Vendor as a material inducement to College and consideration for College entering into the Agreement with Vendor.

Vendor:_____

By: _____

Title: _____

Date: _____