Marshall University
Cloud Computing Contract Addendum

"Institution" as used herein means Marshall University, its Board of Governors, Colleges, Schools, and Departments.

"Vendor" as used herein means _____

(Insert Vendor Name Here)

Definitions

"Confidential Information" is defined as any and all information whose collection, disclosure, protection, and disposition is governed by state or federal law or regulation, particularly information subject to the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), or Marshall University Policy [https://www.marshall.edu/board/board-of-governors-policies/]. This information includes, but is not limited to, Social Security numbers, student records, financial records regarding students (or their parents or sponsors), financial and personal information regarding Marshall University employees, and other personally identifiable information identified by law.

"Covered Data" includes any institutional data defined as "confidential information".

"Institution Data" includes data uploaded by users of the service and communications between the user, the Institution, and Vendor.

"Notification Event" includes Vendor system that may access, process or store University data is subject to unintended access. Unintended access includes compromise by a computer worm, search engine web crawler, password compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.

"Vendor User" includes the Vendor and its employees, agents, contractors, and other persons associated with Vendor.

Use of the Data

The Vendor agrees that data provided to them during the provision of service shall be used only and exclusively to support the service and service execution, and not for any other purpose. Unless expressly permitted by the written consent of an Institution official authorized to give such consent, Vendor and its employees, agents, contractors, and other persons associated with Vendor (collectively, the "Vendor Users") are only permitted to use, reuse, distribute, transmit, manipulate, copy, modify, access, or disclose the Institution Data to the extent necessary for Vendor to implement and maintain the information as set forth in this Addendum. Except as otherwise specifically provided for in this Agreement, the Vendor agrees that Institution Data will not be shared, sold, or licensed with any third-party, except approved sub-contractors, without the express written approval of the Institution and the Senior Vice President for Information Technology.

Vendor will be solely responsible for any unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of Institution data and any non-compliance with the data privacy and security requirements by Vendor Users.

Data Protection

Upon termination, cancelation, expiration or other conclusion of the Agreement, Vendor shall return the Covered Data to Institution unless Institution requests that such data be destroyed. This provision shall also apply to all Covered Data that is in the possession of subcontractors or agents of Vendor. Vendor shall complete such return or destruction not less than thirty (30) days after the conclusion of this Agreement. Within such thirty (30) day period, Vendor shall certify in writing to Institution that such return or destruction has been completed.

Compliance with Federal, State, and Local Laws and Regulatory Requirements; Vendor's product must be compliant with any Federal, State, and Local privacy laws or regulations applicable to the Institution, including but not limited to: the Family Educational Rights and Privacy Act (FERPA) (Pub. L. No. 93-380 (1974), codified at 20 U.S.C. § 1232g); the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. No. 104-191, § 264 (1996), codified at 42 U.S.C. § 1320d; Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160 (2002), 45 C.F.R. § 164 sub pts. A, E (2002); the Gramm-Leach-Bliley Act (GLBA) (Pub. L. No. 106-102 (1999), privacy protections are codified at 15 USC § 6801 et seq.).

Vendor agrees that it may create, have access to, or receive from or on behalf of Institution or students, or have access to, records or record systems that are subject to the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. Section 1232g (collectively, the "FERPA Records"). Vendor represents, warrants, and agrees that it will: (1) hold the FERPA Records in strict confidence and will not use or disclose the FERPA Records except as (a) permitted or required by this Agreement, (b) required by law, or (c) otherwise authorized by Institution in writing; (2) safeguard the FERPA Records according to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which Vendor protects its own Confidential Information; and (3) continually monitor its operations and take any action necessary to assure that the FERPA Records are safeguarded in accordance with the terms of this Agreement. At the request of Institution, Vendor agrees to provide Institution with a written summary of the procedures Vendor uses to safeguard the FERPA Records.

Vendor agrees to adhere to the additional FERPA requirements listed at the following web address: [https://studentprivacy.ed.gov/sites/default/files/resource_document/file/written_agreement_checklist_0.pdf] if any of the data is used for research or a longitudinal study.

Notification of Security Incidents

Vendor, within one day of discovery, shall report to Institution any use or disclosure of Confidential Information not authorized by this Addendum or in writing by Institution. Vendor's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) Confidential Information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Vendor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Vendor has taken or shall take to prevent future similar unauthorized use or disclosure. Vendor shall provide such other information, including a written report, as reasonably requested by Institution.

Vendor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of Vendor's security obligations or other event requiring notification under applicable law ("Notification Event"), Vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the Institution and its Board of Governors, officers, employees, agents and representatives from and against any claims, damages, or other harm related to such Notification Event.

Institutional Marks Protection

Use of Institution name, marks, or logos: All use by Vendor of Institution name, marks, and content must be approved in writing by Institution and the Senior Vice President of Communications. Institution reserves the right to review all uses of its name, marks or logos prior to their use by Vendor.

Indemnification

Vendor shall indemnify, defend and hold Institution harmless from all lawsuits, claims, liabilities, damages, settlements, or judgments, including Institution's costs and attorney fees, which arise as a result of Vendor's negligent acts, omissions or willful misconduct.

ACCEPTED BY:

MARSHALL UNIVERSITY	**VENDOR**
	Company Name: _____
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____