Data Protection Addendum

Personal Data. University of South Alabama ("Client") may from time to time provide _____ (*name of Vendor/Company*) ("Company"), with certain personal data of Client's faculty, employees, students, alumni or other members of the university community, that is regulated by various laws and regulations ("Client Personal Data"). Company confirms that for so long as it processes or is otherwise in possession of Client Personal Data in respect of the relevant Service Agreement or Order Form (or if Company subcontracts certain functions of the service to a 3rd party entity involving the 3rd party's possession of Client Personal Data), Company will adhere to the provisions for the protection of Client Personal Data set forth in the following provisions 1-4, below.

"Client Personal Data" means any electronic data or information submitted by Client to the Company's Cloud Software or Server(s), or in hardcopy form or other means by which Company gains access to the data, that includes a person's name in combination with sensitive ID numbers, or other personal identifiable information (PII). PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an entity intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. For purposes of student information, Client Personal Data will also be construed to include current and past student data that is not included in USA's current Directory Information (see USA's webpage, "FERPA & Your Privacy tab", "What is directory information?").

1. Company confirms that for so long as it processes Client Personal Data in performing its obligations under terms of this agreement, it will:

(a) maintain appropriate technical and organizational data security measures, including a written information security policy to protect the Client Personal Data consistent with applicable federal and state data security and privacy laws and regulations;
(b) maintain the confidentiality of Client Personal Data in accordance with the Service Agreement (or relevant Order Form if applicable);
(c) process the Client Personal Data only in accordance with the Client's instructions; including to process Client Personal Data as reasonably required to perform the obligations described therein. Client hereby authorizes Company to take such steps in the processing of Client Personal Data on behalf of Client as are reasonably necessary for the performance of Company's obligations under the Services Agreement (or Order Form, as applicable).
(d) limit access to the Client Personal Data to Company's employees, agents and subcontractors (including Company's partners or subsidiary companies) who have a need to access such Client Personal Data to perform Company's obligations under this agreement. Client agrees that Company may use subcontractors to fulfill its obligations under this agreement so long as Company's relationship with such subcontractors complies with clause (e) below;
(e) require that its employees, agents and subcontractors who have access to the Client Personal Data agree to abide by substantially similar restrictions and conditions that apply to Company with regard to such Client Personal Data;

(f) implement appropriate administrative, technical and physical safeguards designed to ensure the security or integrity of the Client Personal Data and protect against unauthorized access to or use of such Client Personal Data that could result in substantial harm or inconvenience to the Client;

(g) notify Client of an Information Security Breach as soon as reasonably practicable and without undue delay (but no later than 10 days following the determination of the breach or reason to believe the breach occurred) after Company becomes aware, and take reasonable steps to mitigate the effects of the Information Security Breach, including: (i) provide a list of Client individuals whose data was breached, (ii) identify the types of data breached, and (iii) send breach notification letters to each of the individuals whose personal data was breached to explain what occurred, and include the offer of a 2-year credit monitoring service if they should choose – at no cost to the individual. These steps will enable Client to be compliant with notification requirements per the Alabama Breach Notification Act and any other applicable, similar law or regulation pertaining to individuals who may be protected by other laws (such as other U.S. states, or foreign countries). An "Information Security Breach" is an event that is known to have resulted in unauthorized access to, or unauthorized use or disclosure of, Client Personal Data;

(h) if applicable, will not transfer the Client Personal Data from within the European Economic Area ("EEA") to locations outside the EEA unless it takes such measures as are necessary to ensure the transfer is in compliance with applicable data protection law. Such measures may include (without limitation) transferring the Client Personal Data from a recipient in a country that the European Commission has decided provides adequate protection for personal data, to a recipient that has achieved binding corporate rules authorization in accordance with applicable data protection law, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission.

2. As applicable, the parties may agree to specify the subject-matter and duration of processing of Client Personal Data, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the Client as controller and any specific processing instructions.

3. The parties agree that on the termination or completion of the obligations under this agreement, Company and its subcontractors shall, at the Client's request, return all the Client Personal Data in their possession (if any) and the copies thereof to the Client or shall destroy all the Client Personal Data and certify to the Client that it has done so, unless legal obligations imposed upon Company prevent it from returning or destroying all or part of the Client Personal Data transferred. In the latter case, Company warrants that it will maintain the confidentiality of the Client Personal Data transferred and will not actively process (except for storage and deletion) such Client Personal Data.

4. Company shall have the right to (a) use and otherwise process, and to allow subcontractors/agents to use and otherwise process, Client Personal Data solely for the purposes of performing Company obligations under this agreement and complying with applicable law; and (b) to use and otherwise process Client Personal Data for Company internal business purposes, including development, analysis and corrective purposes in connection with

the Software and Services, and for otherwise improving and enhancing the Software and Services or Company's business, ONLY if the personal data is aggregated / deidentified.

Acknowledged and agreed to by the Parties: The signatures below are expressly authorized by its or their organization as a duly authorized officer and/or party that is authorized to legally sign and bind it's or their company to the terms herein.

CLIENT: University of South Alabama	**COMPANY: (Vendor/Company Name)**
_____	_____
Name	Name
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Title	Title
Email: _____	Email: _____
Date: _____	Date: _____