1. Incorporation by Reference. The Florida Atlantic University Board of Trustees ("FAU") and the undersigned ("Vendor") hereby incorporate this Supplemental Addendum – Privacy and Security ("Addendum") into the agreement between FAU and Vendor (the "Agreement").

2. FAU Data. Under the Agreement, Vendor may access, receive, transmit or maintain non-public data from or on behalf of FAU or its students, employees, or agents. Any such data that Vendor accesses, receives, transmits, or maintains (collectively, "FAU Data") shall be treated as confidential and protected. The term "FAU Data" specifically includes, without limitation, the following data: student information, education records (as defined by 20 U.S.C. § 1232g(a)(4)(A) and 34 CFR § 99.3), Personally Identifiable Information, Protected Health Information, and/or other non-public information, including, but not limited to, metadata, user content, placement information, placement site information, and any communications transmitted or stored in the service.

3. Student Data. Vendor acknowledges that FAU, an educational institution, is subject to legal obligations with respect to the privacy of student information. Vendor acknowledges that the FAU Data may include student education records, as such term is defined under the Family Educational Rights and Privacy Act and regulations promulgated under the Act ("FERPA"). To the extent that FAU Data includes Education Records, Vendor acknowledges and agrees that (i) Vendor shall be deemed to be a "University Official" under FAU's Student Education Records Policy and must abide by the terms and conditions of this Policy and FERPA with respect to Vendor's use and handling of Education Records; (ii) Vendor shall be under FAU's direct control with respect to use and maintenance the handling of Education Records; and (iii) without limiting any other provision of this Addendum, Vendor may not disclose the information to any third party without the prior written consent of the student as required by FERPA. Vendor shall also take any action reasonably requested by FAU to adhere to its obligations under FERPA or otherwise protect the privacy and confidentiality of Education Records.

4. Confidentiality. Vendor agrees (i) to maintain the confidentiality of all FAU Data and to safeguard FAU Data from unauthorized access; (ii) to use the FAU Data solely for the purpose of performing the Services; (iii) to limit disclosure of and access to the information solely to Vendor employees who need to access the information to perform the Services; (iv) to inform these employees of their obligation to maintain the confidentiality of FAU Data; and (v) to not disclose any FAU Data to a third party, except as strictly necessary to perform the Services under the Agreement or otherwise required by law, but only after reasonable prior notice to FAU.

5. Use of Data. Other than as required to perform the Services or its obligations under the Agreement, Vendor shall not contact any individual associated with FAU directly through email or other means, nor shall Vendor cooperate in any way to permit any third party make such contact. Vendor agrees that all FAU Data may only be used expressly and solely for the purpose enumerated in the Agreement and shall not be distributed, repurposed or shaped across other applications, environments, or business units of Vendor, and that no FAU data of any kind shall be transmitted, exchanged or otherwise passed to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by FAU. Within 60 days of termination of the Agreement, Vendor shall destroy the FAU Data or, return the FAU Data to FAU if requested by FAU.

6. Security. Vendor shall utilize all appropriate administrative, physical and technical security measures to ensure the confidentiality, integrity, and security of FAU Data, including, without limitation, industry-accepted fire walls, encryption, current security patches, virus protection measures and access controls. Vendor shall abide by any security measures reasonably requested from time to time by FAU Information Technology Services. FAU reserves the right to modify any FAU information resource, including any software, hardware, or network configuration, in order to protect FAU Data against any security vulnerabilities.

7. Gramm-Leach-Bliley. Without limiting any other provision of this Security Addendum, to the extent that any FAU Data includes customer data as such term is defined under the Gramm-Leach-Bliley Act ("GLB") and the regulations promulgated thereunder, Vendor shall implement and maintain appropriate safeguards to protect this data as required under GLB and the regulations.

8. Credit Card Standards. Vendor shall adhere to all applicable credit card industry requirements, including, without limitation, the Payment Card Industry Data Security Standard (PCI DSS). Vendor is solely responsible for the security of cardholder data in Vendor's possession.

9. Red Flags Rule. To the extent that Vendor has been engaged to provide services with respect to individual financial accounts that are "covered accounts" as defined under 16 C.F.R. § 681.2 (the "Red Flags Rule"), Vendor shall comply with the Red Flags Rule with respect to those covered accounts. Without limiting the foregoing, Vendor shall maintain reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft and to detect Red Flags (as such term is defined in the Red Flags Rule) that may arise in the course of providing the Services. Vendor shall promptly report any Red Flags to FAU and shall take reasonable steps to prevent or mitigate identity theft, including any reasonable steps requested by FAU.

10. GDPR. If FAU Data includes data that is subject to the European Union General Data Protection Regulation (the "GDPR") or if the Services are otherwise subject to GDPR, Vendor shall comply with the GDPR. Without limiting the foregoing, Vendor shall comply with each of the obligations of a "processor" as set forth in the GDPR, including without limitation each of the obligations set forth on the schedule attached hereto (the "GDPR Schedule"). Vendor further agrees that it shall cooperate with FAU in complying with the GDPR, including taking any action reasonably requested by FAU in connection with GDPR obligations.

11. Breaches. If any Vendor has any reason to believe that a breach of this Agreement has occurred or that the security, confidentiality or integrity of any FAU Data could have been compromised or subject to unauthorized access, Vendor shall (a) immediately notify FAU; (b) in cooperation with FAU, take prompt action to thoroughly investigate the incident or potential incident and mitigate any harm flowing from the incident in conjunction with FAU; (c) in cooperation and consultation with FAU, make any required notifications to third parties at Vendor's expense; and (d) take prompt action to prevent any similar incidents from occurring, including, without limitation, the installation of appropriate patches or software within 24 hours of Vendor's discovery of the incident. In the event of material breach of this Addendum by Vendor or a security breach for which Vendor is responsible, FAU shall have the right to terminate the Agreement without penalty upon written notice to Vendor. In the event of either breach, Vendor shall cooperate with FAU in responding to the breach and shall reimburse FAU for any out-of-pocket expenses FAU incurs in its response, including, without limitation, expenses incurred in notifying individuals affected by the breach and/or costs incurred in procuring or providing alternative services.

12. Compliance. Vendor shall comply with all applicable laws, regulations and rules in connection with its access to or handling of FAU Data, including, without limitation, those that are specifically described in this Addendum (collectively, "Applicable Laws"). Vendor shall indemnify and hold FAU, and its trustees, employees, and agents, harmless from any claims, damages, costs, and expenses (including, without limitation, reasonable attorneys' fees) arising out of any failure by Vendor to be in compliance with Applicable Laws or Vendor's breach of this Agreement.

13. Signatures. The parties represent and warrant that any person signing the Agreement has the authority to do so and that such signature shall be sufficient to bind Vendor. The Agreement may be signed electronically and shall be considered signed if/when a party's signature is delivered by facsimile or e-mail transmission of a ".pdf" format date file, including via DocuSign. Such signature shall be treated in all respects as having the same force and effect as an original.

By signing below, Vendor's authorized representative agrees to incorporate this Addendum into the Agreement, and hereby executes this Addendum as of the date set forth below.

VENDOR:

_____

By: _____

Name: _____

Title: _____

Date: _____