Boston College Privacy and Security Addendum

This Addendum by and between Trustees of Boston College ("BC") and _____ ("Service Provider"), amends the agreement between the parties dated _____ (the "Agreement"), under which the Service Provider is providing BC and/or its employees or students with certain services (the "Services").

Under the Agreement, Service Provider may access, receive, transmit or maintain non-public data from or on behalf of BC or its students, employees, or agents. Any such data that Service Provider accesses, receives, transmits or maintains (collectively, "BC Data") shall be treated as confidential and protected as provided in this Agreement. The term "BC Data" specifically includes, without limitation, the following data: _____.

The parties agree as follows:

1. Confidentiality and Use. Service Provider agrees (i) to maintain the confidentiality of all BC Data and to safeguard BC Data from unauthorized access; (ii) to use the BC Data solely for the purpose of performing the Services; (iii) to limit disclosure of and access to the information solely to Service Provider employees who need to access the information to perform the Services; (iv) to inform these employees of their obligation under this Addendum to maintain the confidentiality of BC Data; and (v) to not disclose any BC 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 BC. Other than as required to perform the Services or its obligations under the Agreement, Service Provider shall not contact any individual associated with BC directly through email or other means, nor shall Service Provider cooperate in any way to permit any third party make such contact. Within 60 days of termination of the Agreement, Service Provider shall destroy the BC Data or, if BC requests within this 60 day period, return the BC Data to BC.

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

3. FERPA. Service Provider acknowledges that BC, as an educational institution, is subject to legal obligations with respect to the privacy of student information. Service Provider acknowledges that the BC Data may include personally identifiable student education records ("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 BC Data includes Education Records, Service Provider acknowledges and agrees that (i) Service Provider shall be deemed to be a "University Official" under BC's Student Education Records Policy and must abide by the terms and conditions of this Policy and FERPA with respect to Service Provider's use and handling of Education Records; (ii) Service Provider shall be under BC's direct control with respect to use and maintenance the handling of Education Records; and (iii) without

limiting any other provision of this Addendum, Service Provider may not disclose the information to any third party without the prior written consent of the student as required by FERPA. Service Provider shall also take any action reasonably requested by BC to adhere to its obligations under FERPA or otherwise protect the privacy and confidentiality of Education Records.

4. Massachusetts Data Security Law. If BC Data includes "personal information," as such term is defined in the Massachusetts Security Breach statute (MGL c. 93H), Service Provider shall comply with the such law and the regulations promulgated thereunder (201 CMR 17; "Standards for the Protection of Personal Information of Residents of the Commonwealth"), provided, however, that prior to making any notification to any third party under the statute, Service Provider shall consult with BC and cooperate with BC to determine whether a notification is required and who, as between Service Provider and BC, is required to make the notification.

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

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

7. Red Flags Rule. To the extent that Service Provider 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"), Service Provider shall comply with the Red Flags Rule with respect to those covered accounts. Without limiting the foregoing, Service Provider shall maintain reasonable polices 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. Service Provider shall promptly report any Red Flags to BC and shall take reasonable steps to prevent or mitigate identity theft, including any reasonable steps requested by BC.

8. GDPR. If BC 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, Service Provider shall comply with the GDPR. Without limiting the foregoing, Service Provider 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"). Service Provider further agrees that it shall cooperate with BC in complying with the GDPR, including taking any action reasonably requested by BC in connection with GDPR obligations. .

8. Breaches. If any Service Provider has any reason to believe that a breach of this Agreement has occurred or that the security, confidentiality or integrity of any BC Data could have been compromised or subject to unauthorized access, Service Provider shall (a) immediately notify BC; (b) in cooperation with BC, take prompt action to thoroughly investigate the incident or potential incident and mitigate any harm flowing from the incident in conjunction with BC; (c) in

cooperation and consultation with BC, make any required notifications to third parties at Service Provider'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 Service Provider's discovery of the incident. In the event of material breach of this Addendum by Service Provider or a security breach for which Service Provider is responsible, BC shall have the right to terminate the Agreement without penalty upon written notice to Service Provider. In the event of either breach, Service Provider shall cooperate with BC in responding to the breach and shall reimburse BC for any out-of-pocket expenses BC 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.

9. Compliance with Laws. Service Provider shall comply with all applicable laws, regulations and rules in connection with its access to or handling of BC Data, including, without limitation, those that are specifically described in this Addendum (collectively, "Applicable Laws"). Service Provider shall indemnify and hold BC, 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 Service Provider to be in compliance with Applicable Laws or Service Provider's breach of this Agreement.

10. General. This Addendum shall be effective as of the effective date of the Agreement and shall remain effective so long as the Agreement remains in effect, including during any extensions or renewals of the Agreement. BC or its agents shall have the right, upon reasonable prior notice, to review Service Provider's compliance with this Addendum and its security measures, including the right to have an independent third party conduct a data security audit. Nothing in this Addendum shall limit any of BC's rights or remedies under the Agreement or at law. The terms and conditions of this Addendum shall supersede any conflicting or inconsistent terms and provisions in the Agreement, including all exhibits or other attachments thereto and all documents incorporated therein by reference. Without limiting the foregoing, any limitation or exclusion of damages provisions shall not be applicable to this Addendum.

TRUSTEES OF BOSTON COLLEGE	SERVICE PROVIDER
	_____
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date:_____	Date: _____

GDPR Schedule

This GDPR Schedule sets forth certain obligations of the Service Provider when it is processing personal data on behalf of Boston College and such data is subject to the European Union General Data Protection Regulation ("GDPR"). In connection with such processing, Service Provider shall be deemed a processor under the GDPR and all references to the processor herein shall be a reference to Service Provider. To the extent Boston College is a controller of personal data being processed by Service Provider, then references to the controller herein shall be deemed a reference to Boston College. Terms used in this GDPR Schedule shall have the meaning given to them in the GDPR.

Service Provider agrees that it is obligated as follows:

1. Service Provider has implemented appropriate technical and organizational measures in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of any data subject.

2. Service Provider shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. When processing personal data, Service Provider shall:

   (a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

   (b) ensure that persons authorized to process the personal data, including without limitation Service Provider's employees and contractors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   (c) take all measures required pursuant to GDPR Article 32;

   (d) complies with the conditions referred to in GDPR Article 28, paragraphs 2 and 4 for engaging another processor;

   (e) taking into account the nature of the processing, assist the controller by appropriate technical and organizational measures, to the extent possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights set forth in GDPR Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data;

(h) make available to the controller all information necessary to demonstrate compliance with the obligations set forth in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) above, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

4. If Service Provider engages another processor for carrying out specific processing activities on behalf of Boston College, the same data protection obligations set forth above shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of GDPR. If that other processor fails to fulfil its data protection obligations, Service Provider shall remain fully liable to Boston College for the performance of that other processor's obligations.

5. Service Provider shall maintain a record of all categories of processing activities carried out on behalf of Boston College, in compliance with Article 30(2).

6. Service Provider shall notify Boston College immediately upon becoming aware of any complaint or concern about the Service Provider’s processing activities or compliance with the GDPR.