Rider:
Requirements for the Protection of Harvard
Personally Identifiable Information

As stated in the Purchase Order (in this Rider, the "Agreement"), between the Parties, this Rider is added to and incorporated as part of the Agreement. In the event of any conflict between the terms of this Rider and the Agreement, the terms of this Rider shall govern.

1. For purposes of this Rider, "Personal Data" shall mean any of the following types of personally identifiable information, in any form or media, about current or former Harvard faculty members, employees, students, prospective students, other persons associated with Harvard and other individuals: (i) an individual's social security number, bank or other financial account numbers, credit or debit card numbers, driver's license number, passport number, other government-issued identification numbers, biometric or genetic data, health and medical information, and identifiable data about the individual obtained through a research project (an individual's name together with any of the elements listed in clause (i) is "High Risk Confidential Information"); (ii) identifiable individual financial information, employee benefits information, education records, Harvard identification numbers, and any information about an individual that has been marked as private; and (iii) any additional types of personally identifiable information about individuals that Harvard from time to time designates in writing as Personal Data.

2. In addition to complying with other provisions of the Agreement requiring the protection of confidential information, the Vendor shall:

(i) implement and maintain appropriate security measures for High Risk Confidential Information which shall be at least as protective of the confidentiality of such information as the safeguards for personal information set forth in 201 Code of Massachusetts Regulations 17.00, at all times that such regulations are in effect;

(ii) not use, and not allow the use of, Personal Data for any purpose other than the performance of services for Harvard;

(iii) limit access to Personal Data to Vendor's employees and contractors who have a specific need for such access in order to perform Vendor's services for Harvard (each, a "Permitted Person"), provided that Vendor shall not transfer or give access to Personal Data to any contractor performing the services without Harvard's prior written approval;

(iv) not at any time during or after the term of the Agreement disclose Personal Data to any person, other than Permitted Persons under clause (iii) and Harvard personnel in connection with performance of the services, except with Harvard's prior written consent (or except as required by law, in which case Vendor shall, unless prohibited by law, notify Harvard prior to such disclosure);

(v) obtain written approval from Harvard prior to implementation by Vendor of any remote (including Internet) access to Personal Data by anyone (including any Harvard personnel or students) not a Permitted Person;

(vi) cause all Personal Data to be encrypted when transmitted by Vendor or Permitted Persons via the Internet or any other public network, or wirelessly;

(vii) ensure that Vendor or contractor server computers hosting any Personal Data shall not be directly accessible from the Internet and that access to such servers is secure, and that Personal Data is physically or logically segregated within Vendor's and any contractor's internal data network;

(viii) ensure that Vendor and Permitted Persons (a) do not store High Risk Confidential Information in any portable computing device, for example laptops, tablets, smartphones or similar devices, (b) do not store other Personal Data in any unencrypted portable computing device, and (c) do not store either High Risk Confidential Information or other Personal Data in any external unencrypted portable storage media, for example DVDs, flash drives or backup tapes;

(ix) use measures to protect the security of paper records containing Personal Data while such papers are being stored, used or transmitted that are reasonable in the circumstances, provided that paper records containing High Risk Confidential Information shall be stored in securely locked facilities;

(x) notify Harvard within forty-eight (48) hours of learning of any event that creates a substantial risk of unauthorized acquisition or use of Personal Data or of other harm to any person whose Personal Data is involved in the event, and reasonably cooperate with Harvard in the remediation of such event at Vendor's expense;

(xi) either provide to Harvard on request the results of any SSAE 18 SOC 1 (Type I or Type II) or SOC 2 audit of Vendor's services and system (but Vendor is not obliged hereby to conduct such an audit) or permit an agent of Harvard to conduct such an audit, not more often than annually and at Harvard's expense; and either provide to Harvard on request the results of any vulnerability assessment of Vendor's system or permit Harvard or an agent of Harvard to conduct such tests from time to time, at Harvard's expense;

(xii) comply with such additional protections as Harvard shall reasonably request from time to time in order to comply with any applicable legal requirement; and

(xiii) at any time at Harvard's request and in any case upon termination of the services, return Personal Data to Harvard and (unless otherwise required by law) cause all copies of Personal Data in any formats or media, whether held by Vendor or by a Permitted Person or other person who received Personal Data from Vendor (including Personal Data held in archive or backup files) to be deleted or destroyed, provided that in every case Personal Data shall be disposed of in such a manner that thereafter it cannot practicably be accessed, read or reconstructed from any devices, media or records of any kind held by Vendor or such Permitted Person or other person.

3. With respect to Education Records (as defined below) which Vendor or its Permitted Persons will receive or have access to in connection with Vendor's services, Vendor acknowledges that Harvard has a statutory duty to maintain the privacy of such records and that as a contractor to whom Harvard has outsourced institutional services:

(a) Vendor is performing an institutional service for which Harvard would otherwise use Harvard employees;

(b) Vendor is under the direct control of Harvard with respect to Personally Identifiable Information from Education Records; and

(c) Vendor will comply with all applicable FERPA requirements governing the use and

redisclosure of Personally Identifiable Information from Education Records, including without limitation the requirements of 34 CFR §99.33(a).

"FERPA**"** means the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

*"*Education Records" shall have the meaning given to that term under FERPA and the FERPA Regulations, as amended or otherwise modified from time to time.

"Personally Identifiable Information" from Education Records shall have the meaning given to that term under FERPA and the FERPA Regulations, as amended or otherwise modified from time to time.

4. Vendor shall ensure that applications processing or hosting any Personal Data have been developed and tested to ensure they are free of (i) any viruses, worms or other code or instructions that are constructed to damage, interfere with or otherwise adversely affect computer programs, data files, or hardware, and (ii) the coding deficiencies or vulnerabilities described in: a) the Open Web Application Security Project's (OWASP) "Top Ten Project" – see http://www.owasp.org (as updated from time to time); b) the CWE/SANS Top 25 Programming Errors – see http://cwe.mitre.org/top25/ or http://www.sans.org/top25-programming-errors/ (as each may be updated from time to time); and c) other comparable vulnerabilities generally recognized by the software development/security industry.

5. Vendor shall enforce and be responsible for compliance by all its employees and contractors with the requirements of this Rider and all confidentiality obligations to Harvard.

6. Any provisions of the Agreement that exclude from confidentiality treatment any information that is available to Vendor from third parties, previously known to Vendor, independently developed by Vendor, or not specifically designated as confidential by Harvard, shall be inapplicable to Personal Data.

7. The provisions of this Rider shall survive the termination of the Agreement.