**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, research subjects, other persons associated with Harvard and other individuals: an individual's social security number, tax identification number, military identification number, health insurance identification number, bank or financial account numbers or other identifiable individual financial information, information that would permit access to online accounts, credit or debit card numbers, driver's license number, passport number, other government-issued identification numbers, biometric or genetic data, health and medical information, identifiable data about the individual obtained through a research project, employee benefits information, education records, Harvard identification numbers, any information about an individual that has been marked as private, and 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 Service Provider shall:

(i) implement and maintain reasonable administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of Personal Data which shall be at least as protective of such information as the safeguards for personal information set forth in 201 Code of Massachusetts Regulations 17.00;

(ii) not collect, store, process, transmit or disclose Personal Data or allow such use of Personal Data for any purpose other than the performance of services for Harvard;

(iii) limit access to Personal Data to Service Provider's employees and contractors who have a specific need for such access in order to perform Service Provider's services for Harvard (each, a "Permitted Person"), provided that Service Provider 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 and Harvard personnel in connection with performance of the services, except with Harvard's prior written approval (or except as required by law, in which case Service Provider shall, unless prohibited by law, notify Harvard prior to such disclosure);

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

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

(vii) ensure that Service Provider or contractor computer systems that collect, store, process, or provide access to any Personal Data are secured according to widely used standards such as PCI DSS, ISO 27000, or NIST 800-53;

(viii) ensure that Service Provider and Permitted Persons do not store Personal Data in any unencrypted portable computing device and do not store Personal Data in any unencrypted portable storage media, for example DVDs, flash drives or backup tapes;

(ix) use measures to prevent unauthorized access to paper records containing Personal Data while such papers are being stored, used or transmitted that are reasonable in the circumstances;

(x) either provide to Harvard on request the results of any Service Organization Control Type 2 or 3 (SOC 2 or SOC 3) or equivalent audit of Service Provider's services and system completed within the last 24 months or permit Harvard or its designee 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 Service Provider's system completed within the last 12 months or permit Harvard or its designee to conduct such tests from time to time, at Harvard's expense;

(xi) comply with all applicable data protection laws and regulations, and with such additional protections as Harvard shall reasonably request from time to time in order to comply with any applicable legal requirement;

(xii) immediately notify Harvard if it can no longer meet its obligations under applicable data protection laws and regulations or this Rider; 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 Service Provider or by a Permitted Person or other person who received Personal Data from Service Provider (including Personal Data held in archives or backups) 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 Service Provider or such Permitted Person or other person.

3. Service Provider shall notify Harvard within forty-eight (48) hours of learning of any confirmed or suspected unauthorized acquisition or use of Personal Data or other confirmed or suspected event involving Personal Data ("Security Incident"). Without limiting any other notification obligations of Service Provider under the Agreement, Service Provider shall provide such notice to privsec-incident-report@harvard.edu. In addition, in the event of a Security Incident:

(i) Service Provider shall, at Service Provider's expense, (a) cooperate fully with Harvard to investigate, remediate, and mitigate the effects of the Security Incident, and (b) if requested by Harvard, provide any legally required notifications to affected individuals, government agencies, credit bureaus, and other required entities. Service Provider shall not make any public announcement identifying Harvard or notify affected individuals regarding a Security Incident without Harvard's prior written approval.

(ii) Service Provider shall reimburse Harvard for its third-party costs arising from or related to the Security Incident, including without limitation, costs relating to notifications, credit monitoring, call centers, forensic analyses, fines and penalties, settlements with third parties, and legal and expert advisors.

4. With respect to Education Records (as defined below) which Service Provider or its Permitted Persons will receive or have access to in connection with Service Provider's services, Service Provider 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) Service Provider is performing an institutional service for which Harvard would otherwise use Harvard employees;

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

(c) Service Provider 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.

5. Service Provider 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/ (as may be updated from time to time); and c) other comparable vulnerabilities generally recognized by the software development/security industry.

6. Service Provider shall ensure and be responsible for compliance by all its employees and contractors with the requirements of this Rider and all confidentiality obligations to Harvard. Service Provider shall enter into written agreements with its subcontractors providing for appropriate data protection measures that are at least as restrictive as the terms of this Rider.

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

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