RFP # JL111016 – Appendix C Supplemental Terms and Conditions

Confidentiality Agreement

This Confidentiality Agreement (hereinafter the "Agreement") between the University of Connecticut (hereinafter "UConn" or' "University') and _____ (hereinafter "Contractor) serves to document agreed upon requirements regarding the duty to safeguard Data and Intellectual Property (defined below) that is or may become available to Contractor in the course of providing services to and/or on behalf of UConn. These specifications serve to document agreed upon requirements regarding the duty to safeguard Data and Intellectual Property that is or may become available to Contractor in the course of providing services to and/or on behalf of the University.

Contractor shall comply with the following requirements unless otherwise directed by law or judicial and/or administrative order or prohibited from complying by law or judicial and/or administrative order:

1. **STUDENT DATA.** In the course of performing work for or on behalf of the University, Contractor may have access to data associated with prospective and/or enrolled students. Such information may be subject to the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232g, *et seq*. and the regulations promulgated thereunder at 34 C.F.R. Part 99. Regardless of format or medium (e.g., electronic, paper, audio, video), such information is considered confidential and protected by FERPA. Such information shall not be disclosed or shared with any third party by Contractor, except as permitted by the terms of this Agreement to subcontractors whose services are necessary for Contractor to carry out its services and only then to subcontractors who have agreed to maintain the confidentiality of the data to the same extent required of Contractor under the terms of this Agreement.

   Contractor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all University data received from, or on behalf of the University. These measures shall be extended by contract between Contractor to all subcontractors used by Contractor who may encounter University data.

   In the event any person(s) seek to access protected and confidential data or information, whether in accordance with FERPA or other federal or relevant state law or regulations, that Contractor will promptly inform the University of such request in writing. Contractor shall only retrieve such data or information upon receipt of, and in accordance with, written directions by the University. Contractor shall not provide direct access to such data or information or respond to individual requests. All requests and all data or information retrieved by Contractor in response to such requests shall be provided to the University. It shall be the University's sole responsibility to respond to requests for data or information received by Contractor regarding University data or information. Should Contractor receive a court order or lawfully issued subpoena seeking the release of such data or information, Contractor shall provide immediate notification to the University of its receipt of such court order or lawfully issued subpoena and shall promptly provide the University with a copy of such court order or lawfully issued subpoena prior to releasing the requested data or information.

2. **PERSONALLY IDENTIFIABLE DATA NOT OTHERWISE COVERED BY FERPA.**
   a.) **CONFIDENTIAL DATA.** The data available to Contractor in the course of providing technical support to or on behalf of the University shall be considered Confidential

Information, unless the University indicates otherwise in writing. Such Confidential Information may contain data associated with students, faculty, staff, customers, clients, members of the public, or other individuals affiliated with the University. Information related to such individuals may be protected by federal and/or state laws and regulations, and/or established industry standards. In particular, the contents of such data or information stored and maintained by Contractor may be protected by the Health Insurance Portability and Accountability Act ("HIPAA"), Gramm-Leach Bliley Act ("GLBA"), Electronic Communications Privacy Act (ECPA), federal Red Flags Rule regulations, Federal Trade Commission regulations, Internal Revenue Service regulations and/or other state or federal laws as amended from time to time, and/or by the Payment Card Industry Data Security Standards (PCIDSS), as amended or updated from time to time.

b.) Data or information to which Contractor may become privy in conducting its work for or on behalf of the University shall not be disclosed or shared with any third party by Contractor, except as permitted by the terms of this Agreement or to subcontractors whose services are necessary for Contractor to carry out its services and only then to subcontractors who have agreed to maintain the confidentiality of the data to the same extent required of Contractor under this Agreement.

c.) In the event any person(s) seek to access protected and confidential data or information, such access shall be through the University, and Contractor shall only retrieve such data or information as identified by the University or as otherwise required by federal and/or state law. Contractor shall not provide direct access to such data or information or respond to individual requests.

d.) Should Contractor receive a court order or lawfully issued subpoena seeking the release of such data or information, Contractor shall promptly inform the University of its receipt of such court order or lawfully issued subpoena prior to releasing the requested data or information.

3. **BREACH OF CONFIDENTIALITY.**

The parties agree that any breach of the confidentiality obligations set forth in this Agreement may result in cancellation of this Agreement and/or the ability of Contractor to perform work for or on behalf of the University.

For purposes of this Agreement, "Unauthorized Access," means unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

In the event that a security breach occurs, Contractor agrees to the following:

(1) Contractor shall immediately notify University in the event Contractor has knowledge that Unauthorized Access to Confidential Information has been, or may have been, obtained, and Contractor shall immediately take such measures as are reasonably necessary, or requested by University, to identify the cause, impact and contain such Unauthorized Access (the "Mitigation Measures").

(2) To the extent the Unauthorized Access was not related to the negligent acts or omissions, gross negligence and/or willful misconduct of Contractor and its subcontractors and employees and to Contractor's failure to comply with the terms of this Agreement, Contractor shall, by amendment to this Agreement, be compensated for the Mitigation Measures as an additional service.

(3) To the extent the Unauthorized Access resulted from the negligent acts or omissions, gross negligence and/or willful misconduct of Contractor or its subcontractors or employees, or from Contractor's failure to comply with the terms of this Agreement, Contractor shall (a) be responsible for the costs of the Mitigation Measures; (b) shall take such actions, and be responsible for the costs therefor, as are necessary to mitigate any damage caused, or that may be caused, by such Unauthorized Access, including, but not limited to, providing identity theft protection for a period of not less than two (2) years to those affected or potentially affected by the Unauthorized Access; and (c) shall indemnify and hold harmless the State of Connecticut, including any agency or official of the State of Connecticut, from and against all costs , claims, damages, or expenses, including reasonable attorney's fees, arising from such Unauthorized Access.

4. **NOTIFICATION.** For the purpose of notification to the University of an actual or potential security breach, the following individuals, or their successors, should be contacted, by phone or fax, and also in writing:

- Chief Information System and Security Officer, University Information Technology Services, University of Connecticut, Math Sciences Building, 196 Auditorium Road, Unit 3138, Storrs, CT 06269-3138, Phone: (860) 486-3743, Fax: (860) 486-5744
- Assistant Director of Compliance/Privacy, Office of Audit, Compliance & Ethics, University of Connecticut, 9 Walters Avenue, Unit 5084, Storrs, Connecticut 06269-5084, Phone: (860) 486-5256, Fax: (860) 486-4527

5. **RETURN/DESTRUCTION OF DATA.** Upon expiration or termination of the Agreement, Contractor shall return and/or destroy all data or information received from the University in a manner as may be determined between the parties in accordance with agreed upon standards and procedures. Contractor shall not retain copies of any data or information received from the University once the University has directed Contractor as to how such information shall be returned to the University and/or destroyed. Furthermore, Contractor shall ensure that it disposes of any and all data or information received from the University in the agreed upon manner that the confidentiality of the contents of such records has been maintained. If Contractor destroys the information, Contractor shall provide the University with written confirmation of the method and date of destruction of the data.

6. **PROTECTION OF CONFIDENTIAL INFORMATION.** Contractor agrees that it shall not disclose, provide or otherwise make available proprietary or Confidential Information disclosed to Contractor by the University to any person other than authorized employees, and those employees or agents of Contractor whose use of or access to the Confidential Information is necessary in connection with the work being performed by Contractor for or on behalf of the University. Contractor further agrees that it shall not use Confidential Information for any purpose other than in the performance of the work being conducted for or on behalf of the University. Contractor shall use all commercially reasonable precautions to protect the confidentiality of the Confidential Information, and shall ensure that all employees, agents or contractors of Contractor having access to the Confidential Information understand the commercially reasonable precautions in place, and agree to abide by such precautions.

7. **IDENTITY THEFT PREVENTION.** In an effort to combat identity theft, the University maintains a comprehensive *Identity Theft Prevention Program* with a goal of protecting the personal information of students, employees, affiliates and customers. In the course of performing its duties under this Agreement and through its work for or on behalf of the University, Contractor may collect, access and/or receive personal information pertaining to University students, employees, affiliates and customers that can be linked to

identifiable individuals (hereinafter “Personal Information”). Such Personal Information is Confidential Information of the University. It is the University’s expectation that Contractor will assist the University in its identity theft prevention efforts under *the University’s Identity Theft Prevention Program*. Contractor shall collect, access, receive and/or use such Personal Information solely for the purposes of conducting its work for or on behalf of the University and otherwise in compliance with any and all applicable federal and/or state laws. Additionally, Contractor shall safeguard such information in compliance with all applicable federal and state laws, including but not limited to the Fair Credit Transactions Act of 2003 and any regulations promulgated thereunder (e.g., Red Flags Rule regulations), including implementing appropriate policies or procedures for detecting and identifying possible identity theft and similar fraudulent or potentially fraudulent activities, and notify the University of any such suspicious activities. For the purpose of notification to the University, upon identification of a potential or actual issue of identity theft, Contractor shall immediately contact:

- Assistant Director of Compliance/Privacy, Office of Audit, Compliance & Ethics, University of Connecticut, 9 Walters Avenue, Unit 5084, Storrs, Connecticut 06269-5084, Phone: (860) 486-5256, Fax: (860) 486-4527