Attachment B
UNIVERSITY OF KENTUCKY
Data Privacy and Security Addendum for RFP
UK-2332-23

This Addendum ("***Addendum***"), dated _____, is entered into by and between the UNIVERSITY OF KENTUCKY ("***University***") and _____ ("***Contractor***"). University and Contractor are individually referred to herein as a "***Party***," and together referred to as the "***Parties***."

In consideration of the terms and conditions and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties expressly agree as follows:

1. **Definitions.**

    a. "***Underlying Agreement***" means any contact or agreement into which the Parties have entered or are entering, involving University Data (defined below). This Addendum supplements and is hereby incorporated by reference into the Underlying Agreement.

    b. "***University Data***" means any information, in an electronic, written, or oral form, that Contractor may [create,] obtain, access, transmit, maintain, use, process, store, host and or dispose of on behalf of the University pursuant to the Underlying Agreement. University Data includes, but is not limited to, intellectual property, personal, business, health, financial, and student information, which may include personally identifiable information requiring certain privacy and security protections under federal, state, and/or international law.

2. **Term.** This Addendum shall remain in effect for the term of any attached Underlying Agreement, or any extended term thereto, and any associated scope of work, or for so long as Contractor receives, transmits, processes, stores or otherwise maintains University Data, whichever is longer.

3. **Compliance**. Contractor shall handle University Data in accordance with all applicable state, federal, and international laws, rules, regulations and standards, including without limitation and to the extent applicable, Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, 61.932, and 61.933 ("***Kentucky's Data Security Law***"), Section 255 of the Federal Telecommunications Act of 1996 (47 U.S.C. § 255) and Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194, the Family Educational Rights and Privacy Act ("***FERPA***"), 20 U.S.C. § 1232(g) and 34 CFR Part 99, the Gramm Leach Bliley Act ("***GLBA***"), 5 U.S.C. § 6801 et seq. and the Payment Card Industry Data Security Standard ("***PCI DSS***") (collectively, "***Applicable Law***").

    a. **Kentucky's Data Security Law**. To the extent Contractor receives "Personal Information" as defined by KRS 61.931(6), Contractor shall secure and protect the Personal Information in accordance with Kentucky's Data Security Law by, without limitation: (i) complying with all requirements applicable to non-affiliated third parties set forth in Kentucky's Data Security Law; (ii) utilizing security and breach investigation procedures that are appropriate to the nature of the Personal Information disclosed, at least as stringent as the standards set forth in Section 7(b) below and reasonably designed to protect the Personal Information from unauthorized access, use, modification, disclosure, manipulation, or destruction; (iii) notifying University of a security breach relating to

Personal Information in the possession of Contractor or its agents or subcontractors within seventy-two (72) hours of discovery of an actual or suspected breach unless the exception set forth in KRS 61.932(2)(b)2 applies and Contractor abides by the requirements set forth in that exception; (iv) cooperating with Customer in complying with the response, mitigation, correction, investigation, and notification requirements of Kentucky's Data Security Law, (v) paying all costs of notification, investigation and mitigation in the event of a security breach of Personal Information suffered by Contractor; and (vi) at Customer's discretion and direction, handling all administrative functions associated with such notification, investigation and mitigation.

b. **FERPA**. If Contractor will have access to, store or generate "educational records" as defined by 34 C.F.R. § 99.3, Contractor shall comply with the confidentiality and disclosure restrictions required by FERPA. Contractor agrees that it shall fully comply with all FERPA use and access restrictions applicable to the Underlying Agreement, including but not limited to the restrictions set out in 34 CFR §§ 99.31 and 99.33. Specifically, in performance of its duties, Contractor shall protect data and ensure it is not subject to further disclosure or use. Access shall be strictly restricted to its employees who require access to perform the duties described herein. Contractor shall employ technological access controls to both secure the data from third parties and ensure that it employs effective internal restrictions for access to the records to ensure access and use is limited to the duties described in the Underlying Agreement.

c. **Federal Disabilities Laws**. Contractor warrants that its products or services provided hereunder will be in compliance with all applicable Federal disabilities laws and regulations, including without limitation the accessibility requirements of Section 255 of the Federal Telecommunications Act of 1996 (47 U.S.C. § 255) and Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194. For purposes of clarity, updated regulations under Section 508 standards now incorporate WCAG 2.0 and, for purposes of this Addendum, WCAG 2.0 Level AA compliance is expressly included. Contractor agrees to promptly respond to, resolve and remediate any complaint regarding accessibility of products or services in a timely manner and provide an updated version to University at no cost. If deficiencies are identified, University reserves the right to request from Contractor a timeline by which accessibility standards will be incorporated into the products or services provided by Contractor, and Contractor shall provide such a timeline within a commercially reasonable duration of time. Failure to comply with these requirements shall constitute a material breach of contract and shall be grounds for termination of the Underlying Agreement.

   Contractor will provide University with a current Voluntary Product Accessibility Template (VPAT) for any deliverable(s). If none is available, Contractor will provide sufficient information to reasonably assure the University that the products or services are fully compliant with current requirements.

d. **GLBA**. If Contractor shall receive, maintain, process or otherwise be permitted access to "customer information", as that term is defined in § 314.2(b) of the FTC Safeguard Rule, 16 C.F.R. § 314, and therefore is a "service provider" as defined by 16 C.F.R. § 314.2(d), then Contractor agrees to the following additional terms and conditions:

   (a) Throughout the term of the Underlying Agreement, Contractor shall implement and maintain "appropriate safeguards", as that term is used in §

314.4(d) of the FTC Safeguard Rule, 16 C.F.R. § 314, for all customer information received, maintained, processed, or otherwise accessed by Contractor pursuant to the Underlying Agreement.

(b) Contractor shall notify the University, in writing, of each instance of (i) unauthorized access to or use of any customer information that could result in substantial harm or inconvenience to a customer of the University or (ii) unauthorized disclosure, misuse, alteration, destruction or other compromise of any customer information, within seventy-two (72) hours of occurrence or discovery. Within 30 days of the termination or expiration of the Underlying Agreement, Service Provider shall destroy all records, electronic or otherwise, in its or its agents' possession that contains such customer information and shall deliver a written certification of the destruction to the University.

(c) Contractor consents, upon reasonable advance notice, to University's right to conduct an on-site audit of Contractor's security program.

(d) Notwithstanding any other provisions of this Addendum, University may terminate the Underlying Agreement for cause if Contractor has allowed a material breach of its security program, if Contractor has lost or materially altered customer information, or if the University reasonably determines that Contractor's security program is inadequate.

(e) Contractor shall defend, indemnify, and hold harmless University, its agents, officers, board members, and employees from and against any and all claims, damages, losses, and expenses, including reasonable attorney's fees, for any claims arising out of or in any way relating to any allegations of security breaches, violations of the Safeguard Rule caused by Contractor's negligence, intentional acts or omissions, or any loss or material alteration of customer information.

(f) Contractor shall reimburse the University for any damages, including but not limited to any costs required to reconstruct lost or altered information, resulting from any security breach, loss, or alteration of customer information.

e. **PCI-DSS.** Contractor hereby agrees as follows:

(a) Contractor shall be responsible for the security of cardholder data that it possesses, even temporarily, including any functions relating to storing, processing and transmitting of cardholder data on behalf of the University. For clarity, these functions include the redirection of customers to a third-party service provider website for transaction processing.

(b) Contractor warrants and represents that, as of the effective date of this Addendum, it has complied with all applicable requirements for validation and compliance with the PCI DSS (Payment Card Industry Data Security Standard), as appropriate for its Service Provider level. Contractor agrees to supply the current status of its PCI DSS compliance, and evidence of its most recent validation of compliance, upon execution of the Underlying Agreement. Further, Contractor must supply to the University a new status report and evidence of validation of compliance at least annually and upon request by the University.

Contractor will immediately notify the University if it learns that it is no longer PCI DSS compliant and will immediately report to the University the steps being taken to remediate the non-compliance status. In no event should Contractor's notification to the University be later than seven (7) calendar days after Contractor learns it is no longer PCI DSS compliant. Failure to maintain PCI DSS compliance shall be a breach of contract and the University may, at its sole discretion, terminate the Underlying Agreement if Contractor does not become compliant within thirty (30) days, with any prepaid amounts refunded to University on a pro-rata basis.

(c) If Contractor is providing University with a payment processing system and/or equipment covered by PA DSS (Payment Application Data Security Standard), Contractor warrants and represents that, as of the effective date of the Underlying Agreement, it has complied with all applicable requirements for PA DSS validation for its payment processing system and/or equipment. Contractor agrees to supply evidence of its most recent validation upon execution of this Addendum. Further, Contractor agrees to maintain PA DSS validation for the installed payment processing system version throughout the term of any maintenance agreement with the University. If the PA DSS validation deadline for the payment system lapses, Contractor acknowledges that it shall be in breach of contract and the University may, at its sole discretion, terminate the underlying Agreement if Contractor does not become compliant within thirty (30) days, with any prepaid amounts refunded to University on a pro-rata basis.

(d) While doing business in University facilities or on its property, if credit card payments will be processed over the internet via the Contractor's own system and/or equipment and through its own merchant account, Contractor will provide its own internet connection to process such payments, and will not be permitted to use the University network and equipment.

f. **HIPAA**. The Parties shall enter into a separate Business Associate Agreement ("***BAA***") governing the use or disclosure of any "Protected Health Information" as defined by 45 C.F.R. 160.103, pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA).

4. Rights and License in and to University Data. The Parties agree all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Contractor has a limited, nonexclusive license to use this data as provided in this Addendum solely for the purpose of performing its obligations pursuant to the Underlying Agreement.

5. Permissible Use and Disclosure of University Data.

a. Contractor shall comply with the terms and conditions set forth in this Addendum and the BAA, if any, in its collection, receipt, transmission, access, storage, disposal, use and disclosure of University Data.

b. Contractor agrees to hold University Data in strict confidence and ensure appropriate privacy and security safeguards are in place to prevent the unauthorized use or disclosure of, or unauthorized access to University Data. University Data will not be stored outside

the United States without prior written consent from the University. Contractor shall be responsible for and remain liable to the University for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of University Data under Contractor's control or in its possession.

c. Contractor may use and disclose University Data to those within its organization, any affiliates, subcontractors and agents only to the extent necessary to carry out its obligations to the University under the Underlying Agreement. Contractor will not share University Data with or disclose it to any other third party without the prior written consent of the University, except and to the extent required by law. Contractor shall not disclose University Data to any third party unless and until such third party agrees in writing to be bound by the same restrictions, conditions, and requirements that apply to Contractor under this Addendum and the BAA, if any. Contractor shall be responsible for and remain liable to the University for the actions and omissions of any third parties to whom Contractor discloses University Data as if such were Contractor's own actions and omissions.

6. Security.

a. Contractor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than Contractor uses or would use in good faith to secure its own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

b. Contractor agrees to maintain network security that, at a minimum conforms to one of the following:

i. Current standards set forth and maintained by the National Institute of Standards and Technology, as found at https://nvd.nist.gov; or

ii. Any generally recognized, comparable standard that Contractor then applies to its own network (*e.g.* ISO 27002) and which has been approved in writing by the University.

Contractor shall develop, implement, maintain, update, test annually, and use appropriate administrative, technical and physical security, breach investigation and disaster recovery measures to preserve the confidentiality, integrity and availability of all transmitted and stored University Data received from or on behalf of University. Contractor shall impose these measures on all affiliates and subcontractors used by Contractor.

c. Contractor will be responsible for safekeeping all keys, access codes, combinations, access cards, personal identifying numbers and similar security codes, identifiers, passwords or authenticators issued to Contractor's employees, agents, contractors or subcontractors working with University Data and accounts. Contractor agrees to report a lost or stolen device or information of these employees within 24 hours of such device or information being lost or stolen.

7. Requests for Data, Response to Legal Orders or Demands for Data.
Except as otherwise expressly prohibited by law, Contractor will:

a. immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking University Data; and

b. before making any disclosure of University Data, cooperate with the University's requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request.

8. University's Rights to Information; Audit.

a. Upon University's request, Contractor agrees to provide reasonable documentation to University substantiating compliance by Contractor, its affiliates, subcontractors, and/or agents with Applicable Law, including but not limited to those referenced in Sections 3 of this Addendum.

b. The University may request and obtain access to University Data and related logs at any time for any reason and at no extra cost. The University reserves the right in its sole discretion to perform audits of Contractor at the University's expense to ensure compliance with the terms of the Underlying Agreement and this Addendum. Contractor shall reasonably cooperate in the performance of such audits.

c. Contractor will make itself and any employees, affiliates, subcontractors, and/or agents assisting in the performance of its obligations under the Underlying Agreement, available to the University at no cost to the University. This shall include, without limitation, any data preservation or eDiscovery required by the University or testimony, or otherwise, in the event of litigation or administrative proceedings against University, its directors, officers, agents or employees.

d. Contractor represents and warrants that it maintains adequate internal audit functions to annually assess internal controls in its environment, and to protect the security and confidentiality of University Data. Contractor agrees to provide documentation regarding its internal controls to the University upon request including all internal or external audit reports, certifications, information, documentation, electronic records and data regarding Contractor's internal controls. If requested by University, Contractor will grant University and its University agents or subcontractors, the right to audit Contractor's operations, systems and software to confirm internal controls are present and operating.

e. If the information presented to University regarding Contractor's internal controls is not acceptable to University in its reasonable discretion, Contractor agrees that it will undertake, at its sole cost and expense, an independent SSAE 18 Type II audit or comparable independent attestation to confirm Contractor's controls over its processes. Contractor shall present an action plan acceptable to the University, to correct any and all portions of the systems, software, products, documentation, or internal controls. Contractor shall undertake all activities relating to its preparation of the action plan, and to its correction of any inadequate controls or mitigation of risks revealed by deficiencies in its internal controls at Contractor's sole cost and expense and within a reasonable time period as agreed upon by the University. Should Contractor fail to provide adequate internal controls as described in this Addendum, or to present an action plan acceptable to the University within the mutually agreed upon time frame, University shall be entitled, in its sole discretion, to terminate the Underlying Agreement with no liability whatsoever to

Contractor upon written notice to the Contractor.

9. Security Breach or Incident /Unauthorized Disclosure.

a. Contractor shall immediately and no later than seventy-two (72) hours upon discovery report to University any data breach as defined under any Applicable Law, including without limitation Kentucky's Data Security Law, or any use or disclosure of University Data not authorized by the Underlying Agreement as supplemented by this Addendum or in writing by University ("***Data Incident***"). Contractor's report shall identify: (1) the nature of the unauthorized use or disclosure, (2) the University Data used or disclosed, including a full description of all breached data fields and number of breached records, (3) the identity of the individual(s) or entity that received the unauthorized disclosure, (4) the action(s) that Contractor has taken or shall take to mitigate any potentially negative effects of the Data Incident, and (5) the corrective action(s) Contractor has taken or shall take to prevent future similar unauthorized uses or disclosures.

b. Contractor agrees to cooperate with University and provide reasonable information in its possession or in the possession of any of its affiliates and subcontractors to assist the University in meeting its obligations to investigate and respond to the Data Incident, including allowing University staff to access log information and other pertinent information related to any investigation related to such Data Incident.

c. In the event of a Data Incident within the control of Contractor (or its employees, affiliates, subcontractors, and/or agents involved in performance of Contractor's obligations under the Underlying Agreement) and covered under Kentucky's Data Security Law or other Applicable Law, Contractor shall bear all responsibility and expense for complying with the disclosure and notification requirements under that Applicable Law, except to the extent otherwise authorized in writing by University.

10. Breach of Contract by Contractor. If Contractor has violated a material term of this Addendum and/or the Underlying Agreement or committed gross negligence of its responsibilities to University, the Underlying Agreement may be terminated by the University in accordance with the procedures set forth in the Underlying Agreement.

11. Effect of Termination of Underlying Agreement. Within 30 days upon the termination of the Underlying Agreement for any reason, Contractor shall:

a. Provide University staff with the ability to download and/or export the University Data for records retention purposes.

b. Return or with University's permission destroy all University Data received from University and/or any retained by any of Contractor's affiliates, agents, representatives, or subcontractors, in any form, and Contractor shall retain no copies of such information except and to the extent required by the Underlying Agreement and/or applicable law. If Contractor determines that such return or destruction is not feasible, the protections of this Addendum shall extend to such information and limit further uses and disclosures to those purposes that make the return or destruction of the University Data infeasible, in which case Contractor's obligations under this Addendum shall survive the termination of the Underlying Agreement;

c. Contractor agrees that all paper, film, or other hard copy media shall be shredded or destroyed such that it may not be reconstructed, and University Data shall be purged or destroyed in accordance with NIST Guidelines for media sanitization at http://www.csrc.nist.gov/; and

d. Provide written certification to the University that these actions have been completed.

12. Remedies/Indemnification/Limit of Liability/Insurance.

a. Injunctive Relief. In the event of any breach or violation, or threatened breach or violation, of this Addendum, each Party shall have the right, in addition to any other rights or remedies available, at law or in equity, to seek injunctive relief against the other Party.

b. **Indemnification. In addition to any other remedies available to the University under law or equity, Contractor shall indemnify, defend (to the extent permitted by applicable law), reimburse, and hold University, its affiliates, directors, officers, employees, agents and, if applicable, students (the "Indemnified Parties") harmless from and against all claims, actions, causes of action, demands, liabilities, judgments, fines, assessments, penalties, awards, or other costs and/or expenses, of any kind or nature, including without limitation; those associated with: (i) providing notice to the individuals whose personal information may be impacted by a Data Incident (as described in Section 10 above); (ii) providing any applicable credit monitoring that University may elect in its sole discretion, depending upon the severity of the Data Incident, to provide to the affected individuals or entities, and (iii) legal fees, audit costs, fines and other fees imposed upon any of the Indemnified Parties by regulatory agencies or contracting partners, relating to or arising out of any breach or alleged breach of this Addendum by Contractor, its affiliates or subcontractors.**

c. Insurance. Contractor shall maintain sufficient insurance or financial resources to cover any claims arising from the unauthorized use, disclosure, or breach of, and/or or access to University Data, including without limitation cyber liability insurance in the minimum amount of $1,000,000 and such additional coverages and amounts as expressly agreed to by the Parties in the Underlying Agreement.

13. Conflicts. Any agreements or understandings, whether electronic, click through, verbal or in writing, between (a) Contractor and (b) University (or University employees or other end users) that conflict with the terms of the Underlying Agreement or this Addendum, shall not be valid or binding on the University or any such end users. If there is any direct conflict between this Addendum and the Underlying Agreement, the terms and conditions of this Addendum shall control, unless expressly agreed to in writing by the Parties and signed by an authorized representative of the University.

14. Miscellaneous.

a. Immunity. Nothing in the Underlying Agreement or this Addendum shall be deemed to be a waiver, express or implied, of the privileges and immunities of the University of Kentucky as an agency and instrumentality of the Commonwealth of Kentucky in the United States of America.

b. Changes in the Law. This Addendum shall be deemed amended to conform to any new or revised legislation, rules and regulations to which a Party is subject now or in the future to the extent the new or revised legislation rules and regulations provide more protection to University Data.

c. Waiver. Waiver by University of a breach or violation of any provision of this Addendum will only be effective if done in writing and signed by an authorized representative of the University, and in each case, it will not operate as a waiver of any subsequent or similar breach or violation.

d. Assignment. Neither party may assign this Addendum without the other Party's prior written consent.

e. Survival. Termination or expiration of the Underlying Agreement or this Addendum will not affect the Parties' rights or obligations that, by their nature and context, are intended to survive termination or expiration, including but not limited to those set forth in Section 10, 12 and 13 of this Addendum.

f. Captions. The headings and captions in this Addendum are for reference only and do not and shall not be implied to limit or expand the construction, content and intent of the provisions.

g. Binding Addendum. This Addendum is binding and shall inure to the benefits of the Parties and their respective successors and assigns.

h. Execution and Counterparts. This Addendum may be executed in one or more counterparts, including by fax or by transmission of signed and electronically scanned copies, or via the use of electronic signatures, each of which will constitute an original but all of which together will constitute one and the same Addendum. The Parties acknowledge and agree that this Addendum has been mutually discussed, negotiated, and drafted by the Parties.

This Data Privacy and Security Addendum is executed to be effective as of the date first written above.

UNIVERSITY

By: _____

Printed: _____

Date: _____

CONTRACTOR

By: _____

Printed: _____

Date: _____