

## Data Privacy and Security Addendum

This Addendum (“Addendum”, dated \_\_\_\_\_, is by and between the University of Houston (“*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. University Data:** The Parties acknowledge they have entered or are entering into an Agreement (“Underlying Agreement”) pursuant to which Contractor will create, obtain, access, transmit, maintain, use, process, store, host, and/or dispose of data belonging to the University, such as sensitive 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 (“University Data”). This Addendum supplements and is hereby incorporated by reference into the Underlying Agreement.
- 2. Term.** This Addendum shall in effect for the term of any attached Underlying Agreement, or any extended term thereto, and its 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 and regulations, including but not limited to applicable accessibility requirements such as federal Section 508 Rehabilitation Act requirements (if applicable) and Chapters 206 and 213 of the Texas Administrative Code (the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232(g) and 34 CFR Part 99, the Health Insurance Portability and Accountability Act (“HIPAA”) as set forth at 45 CFR Parts 160 and 164 (“HIPAA”), the Gramm Leach Bliley Act (“GLB”), 5 U.S.C. § 6801 et seq., and the European Union’s General Data Protection Regulation (“GDPR”).
- 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 Agreement solely for the purpose of performing its obligations pursuant to the Underlying Agreement.
- 5. Permissible Use and Disclosure of University Data.** Contractor may use and disclose University Data only to the extent necessary to carry out its obligations to University under the terms of the Underlying Agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by law or permitted in this Addendum.

**6. Privacy.**

- a. 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.
- b. Contractor may only disclose University Data to any affiliates and subcontractors for the purposes set forth in this Addendum and only after the affiliates and subcontractors agree in writing to be bound by the same restrictions, conditions, and requirements that apply to Contractor under this Addendum.

**7. 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
- c. Contractor shall develop, implement, maintain and use appropriate administrative, technical and physical security 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.
- d. 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 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.

**8. 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.

**9. University's Rights to Information.**

- 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 Section 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 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.

**10. Security Breach/Unauthorized Disclosure.**

- a. Contractor shall immediately and no later than 48 hours upon breach discovery report to University any data security breach or any use or disclosure of University Data not authorized by the Underlying Agreement, as supplemented by this Addendum, or in writing by University. 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 unauthorized use or disclosure, 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 incident, including allowing University staff to access log information and other pertinent information related to any investigation related to such breach or unauthorized use or disclosure.
- c. In the event of a security breach or unauthorized disclosure within Contractor's control and covered under the Texas Breach Notification Law (Texas Business and Commerce Code, Chapter § 521) or other applicable laws, Contractor shall bear all responsibility and expense for complying with the disclosure and notification requirements under that statute, except to the extent otherwise authorized in writing by University.

**11. 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.

**12. 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 /export the University Data for records retention purposes.
- b. Return or destroy all University Data received from University and/or any retained by any of its affiliates, agents, representatives, or subcontractors, in any form, and Contractor shall retain no copies of such information; or
- c. If Contractor determines that such return or destruction is not feasible, extend the protections of this Addendum 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;
- d. 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
- e. Provide written certification to the University that these actions have been completed.

**14. Remedies/Indemnification/Limit of Liability/Insurance.**

- a. Injunctive Relief. In the event of any breach or violation, or threatened breach or violation, of this Agreement, 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 (to the extent permitted by applicable law), reimburse, and hold University, its affiliates, regents, 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 sensitive personal information may be impacted by a data security breach or unauthorized use or disclosure of University Data (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 incident, to provide to the affected individuals, 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.

**15. No End User Agreements.** Any agreements or understandings, whether electronic, click through, verbal or in writing, between Contractor and University employees or other end users under this Addendum that conflict with the terms of the Underlying Agreement, including but not limited to this Addendum, shall not be valid or binding on the University or any such end users.

**16. Miscellaneous.**

- a. 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.
- b. Waiver. Waiver by University of a breach or violation of any provision of this Addendum will not operate as a waiver of any subsequent breach.
- c. Assignment. Neither party may assign this Addendum without the other party’s prior written consent.

- d. 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 and 14 of this Addendum.
- e. 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.
- f. Binding Addendum. This Addendum is binding and shall inure to the benefits of the Parties and their respective successors and assigns.
- e. Conflict. If there is any direct conflict between this Addendum and the Underlying Agreement, the terms and conditions of this Addendum shall control.

Executed to be effective as of the date first written above.

**UNIVERSITY**

**CONTRACTOR**

By: \_\_\_\_\_

By: \_\_\_\_\_

Printed: \_\_\_\_\_

Printed: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

*Note: Modification of this Form requires approval from the Office of the General Counsel*