TOWSON UNIVERSITY
CONFIDENTIAL DATA ADDENDUM

EFFECTIVE OCTOBER 1, 2024

Name of Vendor/Contractor:	
TU Contract Number:	
Product or Service:	
Address for Notices and Reports to TU	infosec@towson.edu (or the then-current security email address made available by TU)

THIS ADDENDUM IS HEREBY INCORPORATED INTO THE CONTRACT IDENTIFIED ABOVE ("CONTRACT") BETWEEN THE CONTRACTOR NAMED ABOVE ("CONTRACTOR") AND TOWSON UNIVERSITY ("TU").

1) DEFINITIONS

a. "Appropriate Measures" means compliance with applicable regulatory and industry requirements, as well as best practices for administrative, technical, and physical security controls, provided that in no case shall such measures provide less than equivalent protection to that described in the security standards and controls of NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" (Moderate Baseline).

b. "Confidential Data" includes, but is not limited to, personally identifiable information (as defined in applicable law), including without limitation, name, address, phone number, date of birth, Social Security Number, and student or personnel identification number; FERPA Data (as that term is defined below); cardholder data; biometric information; geolocation data; internet or other electronic network activity information, including IP address; driver's license number; other state or federal identification numbers such as passport, visa, or state identity card numbers; account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; personal health information (as defined in applicable statutes, laws, and regulations); and such other data and information as may be specified by applicable law as "personal data," "personal information," "personally identifiable information" or the equivalent.

c. "TU" means Towson University.

d. "TU Data" means without limitation all information, data, Confidential Data, sound, image, video, derivative products, or other information assets that are provided by or collected on behalf of TU

e. "TU Resources" includes without limitation software, hardware, configurations, and licenses provided by TU

f. "Security Incident" means any actual, suspected, alleged, or potential unauthorized use, access to, disclosure, loss, or alteration of TU Data. Unsuccessful attempts to access information or "pings" on the system do not constitute a Security Incident.

g. "Security Breach" means any "Security Incident" in which it has been confirmed that Confidential Information was accessed by or disclosed to an unauthorized person or party as defined in Md. Code Ann., State Government Article, §10-1301 et seq. ("Protection of Personally Identifiable Information by Public Institutions of Higher Education") and/or all other applicable laws.

2) GENERAL

a. The terms and conditions of this addendum supersede the terms and conditions in any other documents related to this contracted service or the contractual relationship between TU and the Contractor. For purposes of clarity, this includes, but is not limited to, any End User License Agreement ("EULA") or Boilerplate.

applicable to the provision of the services, including payment and PCI-related services or solutions.

3) Contractor agrees to supply the status of Contractor's and Contractor's Third-Party Provider's PCI DSS compliance to TU and evidence of its most recent validation of compliance, upon execution of the Contract and at least annually thereafter.

available to the Contractor pursuant to the Contract is "protected health information" as defined by Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and the rules and regulations promulgated pursuant thereto.

4) SECURITY AND DATA PROTOCOLS

a) Contractor shall support SAML2/Shibboleth or shall provide another method of multi-factor authentication ("MFA"), which alternate method must be acceptable to TU.

b) Contractor represents and warrants that all TU Data shall be stored on servers within the United States. Contractor shall notify TU in writing not less than one hundred and eighty (180) days in advance of any changes in the location of TU Data. If, as a result of the change, TU Data will be stored outside of the United States.

c) Contractor agrees that any transfer of TU Data between TU

2) ISO 27001/2 Certification
3) FedRAMP Authorization

c) If Contractor does not have the reports specified in Section 5(b), then Contractor must submit a Higher Education Cloud Vendor Assessment Tool ("HECVAT") upon execution of the Contract, upon renewal of the Contract, and at other times if requested. If, in its sole discretion, TU believes that Contractor's HECVAT responses do not comply with Appropriate Measures, such non-compliance will be considered a material breach of the Agreement.

d) If Contractor fails to provide any reports required by this Section on the anniversary of the Contract's effective date, such reports shall be provided to TU within thirty (30) days of Contractor's receipt of a written request.

e) Unless waived or amended by TU in writing, Contractor shall perform a formal penetration test on an annual basis. Contractor shall make the results of such tests available to TU each year on the anniversary of the effective date of the Contract.

1) If Contractor fails to provide the penetration test results on the anniversary of the Contract's effective date, such results shall be provided to TU within thirty (30) days of Contractor's receipt of a written request.

2) If a penetration test results in a negative finding, then Contractor shall perform penetration tests at Contractor's expense until the negative finding is resolved.

3) A penetration test means "the process of using approved, qualified personnel to conduct real-world attacks against a system so as to identify and correct security weaknesses before they are discovered and exploited by others."

4) This penetration test must be performed at Contractor's expense by a third-party. The identity of the third party will be disclosed to TU upon request.

6) SECURITY INCIDENT

a) If Contractor becomes aware of a Security Incident, Contractor will notify TU within 48 hours of the time Contractor becomes aware the Security Incident occurred. Notice to TU shall include: 1) the nature and scope of the incident and the affected records or data; and 2) steps that Contractor has taken to mitigate any further incident and prevent further incidents.

b) If the Contractor becomes aware that a Security Breach has occurred, Contractor will provide notice of the Security Breach to TU within 48 hours of the time the Contractor becomes aware the Security Breach occurred. Any breach notifications required by applicable law, including but not limited to FERPA, HIPAA, and Md. Code Ann., State Government §10-13A-03, shall be made in coordination with TU at the Contractor's expense. The Contractor shall not make any notifications without TU's prior written consent.

c) Contractor shall provide access, copies, and/or retrieval, collection, searching, and removal capabilities twenty-four (24) hours a day, seven (7) days a week, with exceptions for scheduled and emergency maintenance. Upon Contractor's receipt of a written request from TU, at Contractor's expense, Contractor will provide TU with any logs, data compilations,

limited to unauthorized disclosure of TU Data, or a fraudulent or unapproved use of PII, PHI, ePHI, EMR, FERPA Data, or credit card information.

b) Contractor acknowledges that any indemnification obligation provided for under the Contract applies also to the failure of the Contractor or any of its subcontractors to be and to remain compliant with the requirements of this Addendum.