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, §10-13A-03 ("Protection of Personally Identifiable Information by Public TUs 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 Agreements, Subscription Agreements, or other terms Contractor may require an end user to accept prior to granting access to and/or use of Contractor products or services.

b. All rights, title, and interest in TU Data and TU Resources shall at all times remain the property of TU. Contractor acquires no rights other than those expressly granted in the Contract.

c. Contractor represents and warrants that, to the best of its knowledge, Contractor's software and all its components do not violate any patent, trademark, trade secret, copyright, or any other right of ownership of any other party.

d. To the extent that assignment, delegation, or subcontracting is permitted by the Contract, Contractor shall contractually require any subcontractors or assignees related to this contract to comply with this Addendum. Contractor shall disclose to TU any subcontractors related to the services to be provided to TU.

e. Contractor shall establish and maintain Appropriate Measures.

f. TU or its auditors shall have the right to audit Contractor's security related to the processing, transport, or storage of TU Data, including, but not limited to, access logs to TU Data.

g. Contractor shall maintain a business continuity plan to address disaster recovery of TU Data and continuity of services to TU. Contractor shall provide satisfactory details of such plan to TU upon request.

h. Contractor shall make available audit logs recording privileged user and regular user access activities, authorized and unauthorized access attempts, system exceptions, and information security events. These audit logs shall be provided in a format that is compatible with industry standard security information and event management system (SIEM) or other audit systems.

i. In connection with the Contract, Contractor may create, host, maintain, and/or receive TU Data from or on behalf of TU and/or its students; and/or have access to, records or record systems containing TU Data.

j. Contractor shall retain TU Data only for the minimum time necessary to complete the work of the Contract and shall delete any TU Data in accordance with NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization, or then-current standards when TU Data is no longer needed.

k. Contractor shall not use, capture, maintain, scan, index, share, mine, process, access, share, sell, disclose, re-release, or distribute TU Data unless:

1) Expressly permitted or required by the Contract, and as necessary to fulfill its obligations under the Contract;

2) Required by applicable law or other legal process; or

3) Otherwise authorized by TU in writing.

l. Upon termination or expiration of the Contract, and at TU's option:

1) Contractor will provide all TU Data to TU. Information must be provided in a format that is acceptable to TU with a data dictionary that enables TU to understand the information provided.

2) Contractor will provide TU with reasonable assistance to transfer the TU Data to an alternate system.

3) Contractor will delete any TU Data in accordance with NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization, or then-current standards.

4) Contractor will return all TU Resources to TU.

m. Contractor shall give TU written notice within forty-eight (48) hours if it receives a subpoena or other governmental request or demand seeking the disclosure of TU Data to allow TU a reasonable amount of time to respond, object, or to otherwise intervene in the action. Contractor will cooperate with TU in any effort to contest such request or demand or to seek a protective order. Contractor agrees that any violation of this review requirement might cause irreparable injury to TU, and that TU will be entitled to injunctive relief, in addition to any other rights and/or remedies provided by the Contract, this Addendum, or applicable law.

3) OBLIGATIONS RELATED TO SPECIFIC TYPES OF DATA

a. **Credit Card Data (PCI–DSS Compliance)**

1) Contractor acknowledges that it is responsible for the security of cardholder data to the extent that Contractor possesses or otherwise stores, processes, or transmits cardholder data on behalf of TU, or to the extent that Contractor can impact or affect the security of the cardholder data environment. Furthermore, Contractor agrees not to introduce, import, or store credit card data within TU's network, thus triggering a requirement for PCI compliance within TU's general network.

2) Contractor affirms that, as of the effective date of the Contract, Contractor and any third-party provider with whom Contractor subcontracts in connection with the Contract ("Contractor's Third-Party Provider") has complied with all applicable PCI requirements, is considered compliant with the Payment Card Industry Data Security Standard ("PCI DSS"), and has performed the necessary steps to validate Contractor's, and, as applicable, Contractor's Third-Party Provider's, compliance with the PCI DSS. Furthermore, Contractor affirms that in any performance hereunder Contractor and Contractor's Third-Party Provider shall remain compliant with all laws and regulations

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.

4) Contractor will immediately notify TU if Contractor learns that Contractor, or Contractor's Third-Party Provider, is no longer PCI DSS compliant, and will immediately inform TU of the steps Contractor is taking to remediate the non-compliance status. In no event should Contractor's notification to TU be later than seven (7) calendar days after Contractor learns Contractor or Contractor's Third-Party Provider is no longer PCI DSS compliant.

5) TU may terminate the Contract immediately without penalty upon notice to the Contractor in the event Contractor, or Contractor's Third-Party Provider, fails to maintain compliance with the PCI DSS or fails to maintain the confidentiality or integrity of any cardholder data.

b. **FERPA Compliance**

1) In connection with the provision of services to TU under the Contract, Contractor may receive, have access to, or store "Education Records," as defined under the Family Educational Rights and Privacy Act ("FERPA") and the regulations promulgated pursuant thereto (all such TU Data hereinafter "FERPA Data").

2) Contractor understands and agrees that TU designates Contractor as a "School Official" with a "Legitimate Educational Interest" in any personally identifiable information contained in the FERPA Data. ("Legitimate Educational Interest" and "School Official" shall have the meanings given to them in FERPA.)

3) Contractor therefore agrees that with respect to all FERPA Data that Contractor creates, hosts, maintains, stores, processes, receives, accesses, or controls, Contractor will comply with all obligations that FERPA imposes on a School Official, including but not limited to the duty:

a) To use the FERPA Data only as necessary to provide services or fulfill its duties under the Contract or as expressly authorized by TU;

b) Not to share, sell, disclose or distribute such FERPA Data to any third party except as expressly provided for in the Contract, required by applicable law, or as otherwise authorized by TU in writing;

c) Not to allow or authorize any of its officers, employees, agents, or subcontractors to access FERPA Data unless and until they have been instructed of their obligations under FERPA and have agreed to comply fully with those obligations; and

d) To retain FERPA Data only as long as necessary to complete the contracted work and to properly destroy FERPA Data in accordance with FERPA.

c. **HIPAA Compliance**

Contractor agrees that it will execute a Business Associate Agreement with TU, if any of the TU Data created, hosted, maintained, stored, processed, or accessed by or otherwise made

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 and the Contractor, or within Contractor's computing environment, will take place using then-current industry standard encryption protocols.

d) Contractor certifies that TU Data will be stored, maintained, and transferred in an encrypted format using at least then-current industry standard encryption practices.

e) Contractor will substantially comply with Open Web Application Security Project ("OWASP") Secure Coding Practices or similar industry secure coding practices.

f) TU shall have the right at all times for any reason whatsoever in its sole discretion, including for purposes of discovery of electronically stored information, to access, retrieve, collect, search, copy and/or remove any or all TU Data at any time. Contractor will aid such access, retrieval, collection, searching, copying and/or removal immediately upon receipt of a written request from TU.

g) **Maryland Law on Protection of Personally Identifiable Information:** As required by Md. Code Ann., State Government Article, Title 10, Subtitle 13 ("Protection of Information by Government Agencies"), and Md. Code Ann., State Government Article, §10-13A-03 ("Protection of Personally Identifiable Information by Public TUs of Higher Education"), Contractor will maintain privacy and security governance programs that conform with the law and support the security and privacy programs of TU.

h) **International Data Privacy Law Compliance:** If any TU Data created, hosted, maintained, stored, processed, or accessed by or otherwise made available to Contractor pursuant to the Contract is subject to international data privacy laws, including but not limited to the EU General Data Protection Regulation, Contractor agrees that it will execute the then-current version of any regulatorily-required standard contractual clauses pursuant to such laws.

5) THIRD PARTY REPORTS

a) TU requires that Contractor provide assurances that Contractor has established and continuously maintains Appropriate Measures in its handling of TU Data.

b) Contractor shall make available a report of a third-party review by a recognized independent audit organization. Such report must be submitted upon granting of the Contract; upon renewal of the Contract; and at other times if requested by TU.

Examples of acceptable control assessment reports include (but are not limited to):

1) AICPA SOC2/Type2

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 re-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. The 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 incidents 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,

or other information or materials applicable to TU within forty-eight (48) hours of the written request.

d) At Contractor's expense, Contractor will cooperate with law enforcement authorities (if applicable) and with TU to investigate a Security Incident and/or Security Breach, and, where necessary, to comply with all applicable legal obligations.

e) TU has the right, in its sole discretion, to terminate the contract in the event of a Security Incident or Security Breach, such termination to be effective immediately upon Contractor's receipt of notice.

f) If the Security Incident resulted from Contractor's or its subcontractor's negligence or breach of the Contract or this Addendum, Contractor shall promptly reimburse all costs to TU arising from such Security Incident, including but not limited to costs for notification and remediation services, the time of TU personnel committed in response to breach, civil and/or criminal penalties levied against TU, attorney's fees, and court costs, etc. This paragraph shall survive the expiration or termination of the contract.

7) INSURANCE REQUIREMENTS

In addition to satisfying TU's standard insurance requirements, Contractor shall obtain and carry the following:

a) **Network Security & Privacy Liability** (also known as Cyber Liability) insurance with limits not less than $3,000,000 for liability and damages resulting from any misuse, misappropriation, unauthorized disclosure or other breach of private information and personally identifiable information, arising from Contractor's performance of services. Such damages shall include notification costs and/or forensics costs, fines, penalties, and related damages.

b) In cases where personally identifiable information ("PII"), personal health information ("PHI"), electronic personal health information ("ePHI"), electronic medical records ("EMR"), or FERPA Data are involved, insurance is required with limits not less than $5,000,000 for liability and damages resulting from any misuse, misappropriation, unauthorized disclosure or other breach of private information and personally identifiable information, arising from Contractor's performance of services. Such damages shall include notification costs and/or forensics costs, fines, penalties, and related damages.

c) This requirement may be satisfied by a stand-alone policy or via Professional Liability/ Technology Errors & Omissions insurance policy. If Network Security & Privacy Liability is included in Contractor's Professional Liability insurance policy, the Network Security & Privacy Liability insurance, including its applicable limit, must be specifically evidenced on the Certificate of Insurance.

8) INDEMNIFICATION

a) Contractor agrees to indemnify and hold TU, the University System of Maryland, and the State of Maryland, and their respective regents, officers, employees, and agents harmless for, from, and against any and all claims, causes of action, suits, judgments, assessments, costs (including reasonable attorneys' fees), and expenses (a) that result from the breach by Contractor or any of its subcontractors of the provisions of this Addendum, or (b) in the event that Contractor's action or inaction permits or results in negligent or malicious activity within Contractor's environment which results in a Security Incident, including but not

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.