ADDENDUM

Terms and Conditions Applying to Third Parties with Michigan Technological University Data

Data Security, Confidentiality, and Breach Handling Requirements Supplement

Revised 01/10/25

All notifications that are required in this Addendum must be sent to MTU Information Security and Assurance at security@mtu.edu, in addition to any other notice addresses in the Order.

1.0 Definitions. When used in this document, the following definitions shall apply:

Addendum – This document and any attachments or materials referenced herein.

Controlled Data – MTU Data that is (i) subject to proprietary rights under patent, copyright, trademark, or trade secret law; (ii) privileged against disclosure in a civil lawsuit (e.g., data subject to attorney-client or doctor-patient privileges); (iii) subject to laws, regulations, rules or standards that prohibit or limit disclosure (e.g., Controlled Unclassified Information ("**CUI**"), the Export Administration Act ("**EAR**"), the Family Educational Rights and Privacy Act ("**FERPA**"), the General Data Protection Regulation ("**GDPR**"), the Genetic Information Nondiscrimination Act ("**GINA**"), the Gramm-Leach-Bliley Act ("**GLBA**"), the Health Insurance Portability and Accountability Act ("**HIPAA**"), the International Traffic in Arms Regulations ("**ITAR**"), and the Payment Card Industry ("**PCI**") data security requirements); or (iv) ought in good faith to be treated as sensitive, proprietary, or confidential.

MTU – Michigan Technological University, including its various campuses, programs, and auxiliary units.

MTU Data – MTU Data includes all information provided directly to Supplier by Michigan Technological University, or information that is created or modified as a result of the product or service being supplied by the Supplier, regardless of presentation format; and may include personal data, operational data, security data, metadata, and user-created content. This data may be Controlled Data (see definition above) and may relate to employees, current students, prospective and former students (alumni), and other affiliates (e.g. volunteers, contractors, etc.).

Order – The contractual agreement, regardless of the title or label used, between the parties by which MTU procures the software, systems, or services from Supplier to which the Addendum is applied and integrated in its entirety.

Supplier – The third-party supplier under the Order.

2.0 Information Security. The terms of this section apply if: 1) MTU is purchasing or leasing software or processing a software renewal; 2) Supplier is creating any computer code for MTU; 3) Supplier receives, processes, stores, or analyzes MTU Data; and/or 4) Supplier is hosting, or managing via infrastructure outside of MTU, including in the cloud, MTU Data.

Supplier shall ensure that all systems or services containing MTU Data are designed, managed, and operated in accordance with information security best practices and in compliance with all applicable laws, rules, and regulations, to include implementation and maintenance of appropriate administrative, technical, and physical safeguards to preserve the confidentiality and integrity of MTU Data. To minimize information security threats, Supplier shall (either directly or through its third-party service providers) meet the following requirements:

a. Access Control. Control access to MTU's resources, including MTU Data, limiting access to legitimate business need based on an individual's job-related assignment. Supplier will approve and track access to ensure proper usage and accountability, and Supplier will make such information available to MTU for review, upon MTU's request.

b. Incident (Breach) Reporting. Report suspected or confirmed information security or privacy incidents within 48 hours of becoming aware to MTU (including those that involve unauthorized disclosure of MTU Data, network intrusions, account compromises involving accounts with access to MTU Data, and unauthorized access or modifications to Supplier systems and applications).

   As soon as practical, but not more than 10 business days after initial notification above, notify MTU whether the breach involved any MTU Data, and if so, provide details on the scope of such a breach including start and end dates, identifying information of natural persons whose data is known or suspected to have been accessed, and any other relevant information. Supplier shall cooperate fully with MTU's investigation of and response to the incident and will remediate any breach subject to applicable laws and regulations.

   Except as otherwise required by law, Supplier shall not provide notice of the incident directly to the natural persons whose MTU Data were involved without prior written notice to and authorization from MTU. In all cases, Supplier will provide copies of any electronic notification to MTU at least 72 hours prior to any planned or anticipated individual notification.

c. Patch and Vulnerability Management. Carry out updates and patch management for all systems and devices in a timely manner and pursuant to reasonable industry best practices.

d. Encryption. All systems, services, and devices that store, process or transmit MTU Data must use an industry standard strong encryption protocol for data in transit and at rest. This requirement extends to backup media containing MTU Data, whether they are logically accessible or not.

e. Regulatory Compliance. When and as applicable, Supplier shall comply with any regulatory requirements for MTU Data provided to Supplier under the terms of the Order, including, but not limited to:

   i. Student Education Records: The Family Educational Rights and Privacy Act ("FERPA"), 20 USC 1232g et seq., and related regulations at 34 CFR Part 99; See Section 6.0 for additional detail.

   ii. Financial Information including credit card and financial account numbers: The Financial Modernization Act of 1999, 15 USC 6803 et seq.; and the Gramm Leach Bliley Act ("GLBA") Safeguards Rule at 16 CFR Part 314.

   iii. Protected Health Information: The Health Insurance Portability and Accountability Act ("HIPAA"), 42 USC 1320d-2; implementing privacy and security regulations at 45 CFR Parts 160 and 164, and related agency guidance.

   iv. Data Protections and Rights for European Union Residents: The General Data Protection Regulation ("GDPR").

f. Security Reviews. If Supplier will store, process, or transmit Controlled Data, Supplier will complete Service Organization Control (SOC) SOC1 or SOC2, Higher Education Cloud Vendor Assessment Tool (HECVAT) Lite or Full, Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CAIQ) or substantially equivalent reviews in accordance with industry standards and provide annually one or more of the above upon MTU's request, as well as at time of Order signing or renewal.

g. Scanning and Penetration Tests. If Supplier will store, process, or transmit Controlled Data, Supplier shall, in accordance with industry standards, perform or engage third party agents or contractors to perform, periodic scans, including penetration tests, for unauthorized applications, hosts, services, code and system vulnerabilities on the networks and systems used by Supplier in the performance of its duties under the Order. All web-based applications (e.g., HTTP/HTTPS accessible Universal Resource Locators (URL)s, Application Program Interfaces (API)s, and web services) should have their own web application security scan and remediation plan as applicable. Supplier must correct weaknesses within a reasonable period, and Supplier must provide proof of testing to MTU upon MTU's request.

h. MTU Right to Audit. MTU reserves the right (either directly or through third party service providers) at its expense to audit all aspects of the Supplier's service, operations, and partners with appropriate confidentiality agreements in place protecting the Provider's intellectual property and/or trade secrets. Notice of intent to audit and negotiation of employee time costs will take place before any audit activity requiring the Supplier. Supplier shall provide MTU reasonable access to any and all necessary files, systems, or reports necessary to conduct any audit permitted under this Addendum. Such access may be at the reasonable times and places specified by Supplier or as may be mutually agreed upon by the parties at the time of the proposed audit.

3.0 Data Confidentiality, Use, Ownership, Disclosure, and Protection. The terms of this section apply if Supplier receives, processes, stores, or analyzes any MTU Data and, to the extent these terms are more restrictive, shall expressly supersede any other terms in the Order or other agreements between the parties.

Confidential Information. For the avoidance of doubt, Confidential Information shall include all MTU Data. Confidential Information does not include information that (a) is known by the receiving party at the time of its receipt, and not through a prior disclosure by the disclosing party, as documented by business records; (b) is published at the time of disclosure, or thereafter becomes published or otherwise part of the public domain without breach of the Order by the receiving party; (c) is subsequently disclosed to the receiving party by a third party who has the right to make such disclosure; (d) is developed by the receiving party independently of Confidential Information or other information received from the disclosing party and such independent development is properly documented by the receiving party; or (e) is required to be disclosed by law or court order.

Data Ownership and Use. MTU Data is MTU's Intellectual Property and Supplier will treat it as confidential information. Supplier will not use, access, disclose, license, or provide to third parties, any MTU Data, except: (i) to fulfill Supplier's obligations to MTU under the Order; or (ii) as authorized in writing by MTU. Where MTU Data is provided to third parties, those third parties must be bound to the terms of the Order or substantially similar terms and conditions. Without limitation, Supplier will not use any MTU Data, whether or not aggregated or de-identified, for product development, training

(whether human or AI), marketing, profiling, benchmarking, or product demonstrations, without, in each case, MTU's prior written consent.

Data Availability, Retention, and Destruction. Upon request by MTU, Supplier will deliver, destroy, and/or make available to MTU any or all MTU Data without charge and without any conditions or contingencies whatsoever. Upon termination of the Order, MTU Data will be returned to MTU in a non-proprietary format that preserves its structure and utility to MTU. Unless otherwise notified in writing, Supplier must destroy all MTU Data on its systems (including subcontractor and agent systems) 60 days after the termination of the Order and provide written certification of destruction to MTU within 10 business days of destruction.

Compelled Disclosure and External Request for MTU Data. Notify MTU immediately if Supplier receives any requests for external release of MTU Data, including, but not limited to, any subpoena for or other legal process or request from a court, governmental authority, or accrediting agency involving MTU Data. This notice must allow MTU sufficient time and opportunity to seek a protective order or to take other appropriate action to protect MTU Data from disclosure.

Data Privacy and Protection. Supplier will ensure that all services undertaken pursuant to the Order are performed in compliance with applicable privacy and data protection laws, rules, and regulations. If Supplier will serve as a Processor of MTU Data that includes Personal Data of Data Subjects who reside in the European Union, Supplier will cooperate with MTU to comply with the GDPR with respect to such Personal Data and Data Subjects. This includes ensuring that all Data Subjects have signed appropriate Consents and signing and complying with all documents and agreements reasonably requested by MTU, including any data processing agreements. All capitalized terms in this section not otherwise defined in the Order will be interpreted as they are defined in the GDPR.

4.0 Payment Card Industry Data Security Standard (PCI DSS). The terms of this section apply if Supplier is processing credit or debit card transactions as part of the Order. For e-commerce business and/or payment card transactions, Supplier will comply with the requirements and terms of the rules of all applicable payment card industry associations or organizations, as amended from time to time (PCI DSS), and be solely responsible for security and maintaining confidentiality of payment card transactions processed by means of electronic commerce up to the point of receipt of such transactions by a qualified financial institution.

Supplier will, at all times during the Order, be in compliance with the then current standard for Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA DSS) for software, and PIN Transaction Security (PCI PTS) for hardware. Supplier will provide attestation of compliance to MTU annually by delivering to MTU current copies of the following: (i) Supplier's "Attestation of Compliance for Onsite Assessments – Suppliers;" (ii) an attestation that all MTU locations are being processed and secured in the same manner as those in Supplier's "PCI Report on Compliance;" and (iii) a copy of Supplier's PCI Report on Compliance cover letter. Supplier will notify MTU immediately if Supplier becomes non-compliant, and of the occurrence of any security incidents.

Supplier's services must include the following:

a. Supplier maintains its own network operating on its own dedicated infrastructure. Supplier's network includes a firewall that (i) includes access control rules that separate Supplier's PCI network from MTU, and (ii) restricts any communication between Supplier's network devices and MTU systems.

b. Supplier treats the MTU network as an untrusted network and no unencrypted cardholder data traverses or otherwise is stored on MTU's network, and MTU has no ability to decrypt cardholder data.

c. All devices must be Secure Reading and Exchange of Data) (SRED); Europay, MasterCard and VISA (EMV); and Payment Card Industry Point of Interaction (PTS POI) compliant.

5.0 Privacy; Educational Records. Student educational records are protected by the U.S. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA). Supplier will not require any MTU students or employees to waive any privacy rights (including FERPA or the European Union's GDPR or other similar extraterritorial privacy laws) as a condition for receipt of any educational services, and any attempt to do so will be void.

Supplier will comply with FERPA and will not access or disclose student educational records to third parties without prior notice to and consent from MTU or as otherwise provided by law. If the Order contains a scope of work or other provision that requires or permits Supplier to access or release any student records, then, for purposes of the Order only, MTU designates Supplier as a "school official" for MTU under FERPA, as that term is used in FERPA and its implementing regulations. In addition, any access or disclosures of student educational records made by Supplier must comply with MTU's definition of legitimate educational interest (included within MTU's FERPA disclosure notice located at [1]). If Supplier violates the terms of this section, Supplier will immediately provide notice of the violation to MTU.

6.0 Export Control. The terms of this section apply if Supplier expects to store, process, or transmit export-controlled data. Supplier hereby certifies that it will comply with all U.S. export control laws and regulations including but not limited to the International Traffic in Arms Regulations ("ITAR") (22CFR 120-130), Export Administration Regulations ("EAR") (15CFR 730-774) and regulations administered by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") (31CFR 500-598). The Supplier will receive, store, process, and analyze MTU Data only within the borders of the United States of America (USA) unless otherwise authorized by MTU in writing. Export controlled software or MTU Data will at all times reside in the USA and only be accessible to Supplier personnel physically located within the USA.

7.0 Controlled Unclassified Information (CUI). The terms of this section apply if Supplier expects to store, process, or transmit controlled unclassified information (CUI) or Security Protection Data (SPD) on behalf of MTU or is later determined to do so. Supplier attests that it 1) is FedRAMP authorized; or 2) that its service meets relevant control requirements as contained in the current version of NIST SP 800-171; or 3) commits to resolving any NIST SP 800-171 control deficiencies within six (6) months of notification by MTU that it must comply with NIST SP 800-171 controls. Failure to provide a NIST SP 800-171 compliant solution within the notice period shall be grounds for MTU to terminate the Order without penalty, including prorated refunds when applicable.

8.0 Accessibility. The terms of this section apply if: 1) MTU is purchasing or leasing software or processing a software renewal; 2) Supplier is creating any computer code for MTU. Electronic applications and websites ("computer code") created or maintained by Supplier on behalf of MTU and intended for MTU student or employee access must comply with Section 504 of the Rehabilitation Act of 1973 (29 USC 794 and its implementing regulations at 34 CFR Part 104) and with Title II of the Americans with Disabilities Act of 1990 (42 USC 12131 and following and implementing regulations at 28 CFR Part 35). Information and communication technologies (ICT), including websites, must conform with the best practices including criteria defined in the W3C's Web Content Accessibility Guidelines (WCAG) 2.0 Level AA and the Web Accessibility Initiative Accessible Rich Internet Applications Suite (WAI-ARIA) 1.0 techniques for web content.

9.0 Conflict Resolution. In the event any provisions embodied in this Addendum are found to conflict with other contractual language the Order, or in other applicable and relevant agreements between the parties, the more restrictive provisions will apply.

[1] - https://www.mtu.edu/policy/policies/general/1-11/