

UNIVERSITY OF MARYLAND, COLLEGE PARK SENSITIVE AND SECURE DATA ADDENDUM

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

THIS ADDENDUM IS HEREBY INCORPORATED INTO THE CONTRACT IDENTIFIED ABOVE ("CONTRACT") BETWEEN THE CONTRACTOR NAMED ABOVE ("CONTRACTOR") AND UNIVERSITY OF MARYLAND ("UMD").

1) DEFINITIONS

- a. "Appropriate Measures" shall mean compliance with applicable regulatory and industry requirements, as well as best practices for administrative, technical, and physical security controls; *provided however*, 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. "Security Incident" means any actual, suspected, alleged, or potential unauthorized use, access to, disclosure, loss, breach, or alteration of UMD Data. Unsuccessful attempts to access information or "pings" on the system do not constitute a Security Incident.
- c. "UMD Data" means without limitation all information, data, personal data, sound, image, video, or other files, including applications, that are provided to, uploaded to, stored, or otherwise accessible by Contractor pursuant to or in connection with the Contract.

Personal 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.

- d. “UMD Resources” includes without limitation software, hardware, configurations, and licenses.

2) GENERAL

- a. All rights, title, and interest in UMD Data and UMD Resources shall at all times remain the property of UMD. Contractor acquires no rights other than those expressly granted in the Contract.
- b. Upon termination or expiration of the Contract, all UMD Resources shall be restored to UMD.
- 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 providing services to UMD pursuant to the Contract to comply with this Addendum. Contractor shall disclose to UMD any subcontractors related to the services to be provided to UMD.
- e. Contractor shall establish and maintain Appropriate Measures, to protect against:
 - 1) Unauthorized access to, or destruction, loss, or alteration of the UMD Data or UMD Resources; and
 - 2) Interruptions to services and/or unavailability of materials provided pursuant to the Agreement, subject to any limitations described in the Agreement.

For purposes of clarity, paragraphs 1) and 2) are exemplary risks, the inclusion of which does not limit the applicability of the Appropriate Measures to protect against other risks.
- f. UMD or its auditors shall have the right to audit Contractor’s security related to the processing, transport, or storage of UMD Data.
- g. Contractor shall maintain a business continuity plan to address disaster recovery of UMD Data. Contractor shall provide satisfactory details of such plan to UMD upon request.
- h. Contractor shall ensure continuity of services in the event of Contractor being acquired or a change in Contractor’s management.
- i. Notwithstanding anything in the Contract to the contrary:
 - 1) Contractor shall not have the unilateral right to limit, suspend, or terminate the service (with or without notice and for any reason); and
 - 2) Contractor shall not disclaim liability for third-party action or negligence.

- j. Contractor shall make available audit logs that include, but are not limited to, the recording of privileged user and regular user access activities, authorized and unauthorized access attempts, system exceptions, and information security events (as available).

3) UMD DATA

- a. In connection with the Contract, Contractor may: create, host, maintain, receive UMD Data from or on behalf of UMD and/or its students; and/or have access to, records or record systems containing UMD Data.
- b. Contractor shall not use, access, share, sell, disclose, re-release, or distribute UMD 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 UMD in writing.
- c. Contractor shall not allow or authorize any officers, employees, agents, or subcontractors of Contractor to access or use UMD Data unless they have agreed to comply fully with the obligations imposed by the Contract and this Addendum.
- d. Contractor shall safeguard UMD Data using Appropriate Measures.
- e. Contractor shall maintain the confidentiality of all UMD Data using at least the same standard of care it uses to protect its own confidential or proprietary information but, in any event, no less than Appropriate Measures.
- f. Contractor shall not capture, maintain, scan, index, share or use any UMD Data for any non-authorized activity. For purposes of this requirement, “non-authorized activity” means data mining or processing of data, stored, or transmitted by Contractor, for any purpose (other than providing the services to UMD) that is not explicitly authorized in the Contract or under applicable law.
- g. Upon termination or expiration of the Contract, and at UMD’s option, (a) Contractor will provide UMD with reasonable assistance to transfer the UMD Data to an alternate system, or (b) Contractor shall delete any UMD Data and shall restore the UMD Data to UMD. Any deletion of UMD Data must comply with NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization, or then-current standards.

4) 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 UMD, 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 UMD’s network, thus triggering a requirement for PCI compliance within UMD’s general network.

- 2) Contractor affirms that, as of the effective date of the Contract, it and any third-party provider with whom it subcontracts in connection with the Contract 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 its compliance with the PCI DSS. Furthermore, Contractor affirms that in any performance hereunder it and any third-party provider with whom it subcontracts in connection with the Contract shall remain compliant with all laws and regulations applicable to the provision of its services, including payment and PCI-related services or solutions.
- 3) Contractor agrees to supply the current status of Contractor’s PCI DSS compliance status to UMD, and evidence of its most recent validation of compliance, upon execution of the Contract.
- 4) Contractor will immediately notify UMD if it learns that it is no longer PCI DSS compliant, and will immediately inform UMD of the steps it is taking to remediate the non-compliance status. In no event should Contractor’s notification to UMD be later than seven (7) calendar days after Contractor learns it is no longer PCI DSS compliant.
- 5) UMD may terminate the Contract immediately without penalty upon notice to the Contractor in the event Contractor 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 UMD 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 UMD Data hereinafter “FERPA Data”).
- 2) Contractor agrees to comply with this Addendum in connection with its use, storage, and acquisition of FERPA Data.
- 3) Contractor understands and agrees that UMD 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.)
- 4) 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 UMD;
 - 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 UMD 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;
- d) To store, manage, and/or destroy FERPA Data in accordance with FERPA; and
- e) Only to re-disclose, manage and/or destroy FERPA Data in aggregated, de-identified forms as authorized under FERPA.

c. **HIPAA Compliance:**

Contractor agrees that it will execute a Business Associate Agreement with UMD, if any of the UMD 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.

5) SECURITY AND DATA PROTOCOLS

- a) Contractor shall develop, implement, maintain, and use Appropriate Measures to preserve the confidentiality, integrity, and availability of all electronically maintained or transmitted data received from, or on behalf of UMD or its students, including without limitation UMD Data.
- b) Contractor shall support SAML2/Shibboleth, or shall provide another method of multi-factor authentication (“MFA”), which alternate method must be acceptable to UMD.
- c) Contractor represents and warrants that all UMD Data shall be stored on servers within the United States. Contractor shall notify UMD in writing not less than one hundred and eighty (180) days in advance of any changes in the location of UMD Data if, as a result of the change, UMD Data will be stored outside of the United States.
- d) Contractor agrees that any transfer of UMD Data between UMD and the Contractor, or within Contractor’s computing environment, will take place using then-current industry standard encryption protocols.
- e) Contractor certifies that UMD Data will be stored and maintained in an encrypted format using at least then-current industry standard encryption practices.
- f) Contractor will use only Appropriate Measures to access and electronically transfer UMD Data files to/from UMD and/or the Contractor.
- g) Contractor will substantially comply with Open Web Application Security Project (“OWASP”) Secure Coding Practices.
- h) Contractor shall give UMD written notice within forty-eight (48) hours if it receives a subpoena or other governmental request or demand seeking the disclosure of UMD Data in order to allow UMD a reasonable amount of time to respond, object, or to otherwise intervene in the action. Contractor will cooperate with UMD 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 UMD, and that UMD will be entitled to injunctive relief, in addition to any other rights and/or remedies provided by the Contract, this Addendum, or applicable law.

- i) Prior to a proposed production of any UMD Data, Contractor and UMD shall agree on the costs of production.
- j) UMD 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 UMD Data at any time. Contractor will aid such access, retrieval, collection, searching, copying and/or removal immediately upon receipt of a written request from UMD.
- k) 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 UMD, at Contractor's expense, Contractor will provide UMD with any logs, data compilations, or other information or materials applicable to UMD within forty-eight (48) hours of the written request.
- l) **Maryland Law re Protection of Personally Identifiable Information:** Contractor will maintain a privacy governance program that substantially conforms to the requirements of 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 Institutions of Higher Education*").
- m) **International Data Privacy Law Compliance:** If any UMD 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.

6) THIRD PARTY REPORTS

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

If Contractor is handling payment card data, then Contractor must supply UMD with a new status report and evidence of validation of PCI compliance (an "Attestation of Compliance" or "AOC") at least annually.

- 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 UMD.

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 6(b), then Contractor must submit a Higher Education Cloud Vendor Assessment Tool (“HECVAT”) upon execution of the Agreement, upon renewal of the Agreement, and at other times if requested. If, in its sole discretion, UMD 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 UMD within thirty (30) days of Contractor’s receipt of a written request.
- e) Contractor shall perform a formal penetration test on an annual basis. Contractor shall make the results of such tests available to UMD 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 UMD 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 which will be disclosed to UMD upon request.

7) SECURITY INCIDENT

- a) If Contractor becomes aware of a Security Incident, Contractor will immediately notify UMD, and will provide any other notifications required by applicable law and requirements, including without limitation PCI DSS requirements, FERPA, and HIPAA.
- b) Notice shall include:
 - 1) The nature and scope of the breach and the affected records or data; and
 - 2) Steps that Contractor has taken to mitigate any further breach and prevent further breaches.
- c) At Contractor’s expense, Contractor will cooperate with law enforcement authorities (if applicable) and with UMD to investigate a Security Incident and, where necessary, to comply with all applicable legal obligations, including but not limited to all applicable laws and/or regulations governing breach notification (including paying costs of notification and remediation); *provided, however*, that Contractor shall not make any such notifications without UMD’s prior written consent.
- d) Contractor shall comply with any UMD requests to notify those affected by the Security Incident at Contractor’s expense.

- e) UMD has the right, in its sole discretion, to terminate the contract in the event of a Security Incident, 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 UMD arising from such Security Incident, including but not limited to costs for notification and remediation services, the time of UMD personnel committed in response to breach, civil and/or criminal penalties levied against UMD, attorney's fees, and court costs, etc.

8) INSURANCE REQUIREMENTS.

In addition to satisfying UMD'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 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 is required. 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.

9) INDEMNIFICATION

- a) Contractor agrees to indemnify and hold UMD, the University System of Maryland, and the State of Maryland, and their respective regents, officers, employees, and agents and 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 UMD Data, or a fraudulent or unapproved use of PII, PHI, ePHI, EMR, FERPA Data, 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.

a.