APPENDIX D

PRIVACY AND SECURITY

Revised: February 1, 2024

1. Data Privacy

a. Contractor will use data either supplied by University or to which Contractor has access to under the Agreement, including without limitation University Education Records (as defined below), Contractor University Data (as defined below) and Nonpublic Customer Information (as defined below), (collectively "SUNY Data") only for the purpose of fulfilling its duties under the Agreement for University's benefit and will not share SUNY Data with or disclose it to any third party without the prior written consent of University, except as required by the Agreement or as otherwise required by law. Contractor may disclose SUNY Data to the extent that disclosure is based on the good-faith written opinion of Contractor's legal counsel that disclosure is required by law or by order of a court or governmental agency. Contractor may exercise this right only if it has requested this disclosure and communicated the legal opinion in writing and in advance to the University. For clarity, SUNY Data does not include information provided directly to Contractor by Contractor-Identified Students or their representatives or that is not contained in an application to the University.

b. All SUNY Data shall be considered to be confidential and shall be treated as such by Contractor, its employees and subcontractors. Contractor shall implement and maintain appropriate policies and procedures to safeguard the confidentiality of SUNY Data in accordance with the Agreement. Contractor shall notify University promptly of any requests, from any source, for copies of or access to, or other disclosure of SUNY Data. If there is an actual or reasonably suspected accidental, unauthorized, impermissible, or unlawful disclosure, use, access, alteration, loss, or destruction of SUNY Data ("Information Security Incident"), Contractor shall notify the University in accordance with Section 9 of this Appendix and immediately take all appropriate steps to mitigate any potential harm or further accidental, unauthorized, impermissible, or unlawful disclosure, use, access, alteration, loss, or destruction of such SUNY Data. Upon University's request and at the cost of Contractor, Contractor shall also cooperate with and assist University with any notifications required by applicable laws or regulations or requested by University relating to any Information Security Incident, which may include without limitation notifying affected persons and relevant legal authorities on behalf of University. Upon the expiration or termination of the Agreement, and at any other time at the written request of the University, Contractor shall promptly return to the University all SUNY Data (and all copies of this information) that is in Contractor's or any of its subcontractor's possession or control, in a form useable and agreeable to University. If return of SUNY Data is not feasible, Contractor may, subject to University's written consent, destroy such information provided Contractor provides University with a certificate confirming date of destruction of such data.

c. SUNY Data must be stored, housed, processed, backed-up, archived and otherwise retained on systems physically located in the continental United States, unless an exception is explicitly approved in writing by University. This requirement applies to all of Contractor's subcontractors.

Signing of the Agreement is not considered explicit approval in writing by University.

d. Contractor will provide access to SUNY Data only to its employees and subcontractors who need to access the SUNY Data to fulfill Contractor's obligations under the Agreement.

e. Contractor will ensure that employees and subcontractors who perform work under the Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of the Agreement. Contractor's employees and subcontractors who may access SUNY Data must have executed agreements concerning access protection and data/software security that are consistent with the terms and conditions of the Agreement prior to being provided such access and which require them to comply with all University, Stony Brook University Hospital or State University of New York policies and procedures regarding data access, privacy and security, including those prohibiting or restricting remote access to University's systems and data.

f. Privacy Notification

i) The authority to request the personal information described under Section 5.4 of **Appendix A** to the Agreement from a seller of goods or services or a lessor of real or personal property, and the authority to maintain such information, is found in Section 5 of the New York State Tax Law. Disclosure of this information by the seller or lessor to SUNY or the State is mandatory. The principal purpose for which the information is collected is to enable the State to identify individuals, businesses and others who have been delinquent in filing tax returns or may have understated their tax liabilities and to generally identify persons affected by the taxes administered by the Commissioner of Taxation and Finance. The information will be used for tax administration purposes and for any other purpose authorized by law.

ii) The personal information is requested by the purchasing unit of SUNY contracting to purchase the goods or services or lease the real or personal property covered by this contract or lease. The information is maintained in the Statewide Financial System by the Vendor Management Unit within the Bureau of State Expenditures, Office of the State Comptroller, 110 State Street, Albany, New York 12236.

2. Family Educational Rights and Privacy Act ("FERPA")

a. Contractor may have access to Education Records as defined under the Family Educational Rights and Privacy Act ("FERPA") and its implementing regulations which includes any data provided to Contractor by University's students for the purpose of fulfilling the terms of the Agreement (collectively "University Education Records"). Contractor acknowledges that for the purposes of the Agreement it will be designated as a "school official" with "legitimate educational interests" in the University Education Records and Contractor shall abide by the limitations and requirements imposed on school officials under FERPA with respect to the University Education Records.

3. Data Security

a. Contractor shall maintain, during the term of the Agreement, network security which includes: network firewall provisioning, intrusion detection, and regular third party vulnerability assessments, and share such assessment results with University. Contractor shall maintain network security that conforms to generally recognized "Industry Standards "and best practices and University security policies (https://it.stonybrook.edu/policies), procedures and requirements. Generally recognized industry standards include, but are not limited to, the current standards and benchmarks set forth and maintained by the Center for Internet Security (see http://www.cisecurity.org) or Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org/

b. Contractor shall implement and use network management and maintenance applications and tools, appropriate intrusion prevention and detection, and data confidentiality / protection / encryption technologies for endpoints, servers and mobile devices. This must include mechanisms to identify vulnerabilities and apply security patches. Contractor will also physically and logically separate different customers' networks where applicable.

c. Contractor shall establish, maintain, and provide documentation of a continuous security program throughout the term of the Agreement ("Data Security Program"). The Data Security Program shall comply with PCI DSS requirements and all applicable legal and regulatory requirements for data protection. In addition, the Data Security Program will protect against any anticipated threats or hazards to the security or integrity of information stored on its servers and unauthorized access to or use of such information that could result in harm or inconvenience to the person who is the subject of such information. Contractor will review, at least annually, its Data Security Program and update and revise it as needed. The Contractor will provide information in the form requested by University, including but not limited to the completion of a security questionnaire and relevant diagrams and/or whitepapers. The Data Security Program must enable University (or its selected third party) to:

i) Define the scope and boundaries, policies, and organizational structure of an information security management system.
ii) Conduct periodic risk assessments to identify the specific threats to and vulnerabilities of University.
iii) Implement appropriate mitigating controls and training programs, and manage resources.
iv) Monitor and test the Data Security Program to ensure its effectiveness. Contractor shall review and adjust the Data Security Program in light of any assessed risks.

d. In no event shall Contractor's action or inaction result in any situation that is less secure than the greater of:

i) The security that University provided as of the date of the Agreement.

ii) The security that Contractor then provides for its own systems and data.
iii) Contractor will provide access of any third-party certifications held, including but not limited to SOC II, FedRAMP, ISO2700 or PCJ.

e. Contractor shall ensure physical security of SUNY Data. This includes:

i) Physical access to any equipment that contains any SUNY Data.
ii) Any mobile storage devices, laptops, or any other access on desktops that allow Contractor's employees or subcontractor's to access, transmit, or store. These devices must be encrypted and employ appropriate authentication mechanisms to assure access is limited to authorized individuals (e.g. two factor authentication.)
iii) Scenarios for moving and storing electronic data off-site in a secure manner.
iv) Physical Transport of Data- Contractor shall use reputable means to transport data. Deliveries must be made either via hand delivery by an employee of the Contractor, by reputable moving company complying with University specified security measures or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor's offices, to and from subcontractors, and to the University.

f. Contractor shall, upon request:

i) Complete and submit the appropriate version of the Higher Education Community Vendor Assessment Tool (HECVAT).
ii) Complete a SOC 2 Type 2 report, or equivalent, recognized information security audit report performed by an independent, certified 3rd party auditor covering the principles of Security, Availability, Confidentiality, and Privacy. The equivalent audit report must be based on a recognized information security standard.
iii) Address the ability to provide the same levels and types of security through multiple data access methods (e.g., Web, mobile devices, or network).

Both the HECVAT and SOC 2 Type 2 report must be completed by the appropriate experts in this area.

g. University will authorize, and Contractor will issue, any necessary information access mechanisms, including access identities (IDs) and passwords, to be used by Contractor and its employees and subcontractors. Contractor shall provide these individuals with only the minimum level of access necessary to perform the tasks and functions for which they are responsible under the Agreement. Contractor shall update, as necessary, a list of those employees and subcontractors of Contractor who have access to University's systems, software and SUNY Data, and the level of such access. Remote access for support to resources on-

premise at University will be granted only through methods approved by University. Access will be limited to named individuals and require logging and security controls that will assure access is limited to authorized individuals (e.g. two factor authentication). These logs will be provided to University upon request.

h. University and Contractor will collaborate on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures, set escalation thresholds, and conduct training. Contractor shall, at the request of University, and, quarterly, provide University Information with a report of the incidents that it has identified and take measures to resolve.

4. Data Portability

a. Contractor agrees that University owns SUNY Data and that Contractor will take all steps and actions, at the direction of University, that are necessary and reasonable to facilitate and complete the orderly, efficient, expedient and professional transfer of the Services and SUNY Data, in whole or in part, in the format and on the media requested during the Term and/or upon the expiration or termination of the Agreement to University, a University Institution, or third-party that University may select. The cost of any such transfer services shall be borne by Contractor.

5. Contractor Personnel

a. If consistent with Contractor's employment policies, Contractor shall conduct a drug screening and background check on all individuals that Contractor provides access to SUNY Data and review the results of such screening and check of each person to verify that the person meets the Contractor standards for employment.

6. New York Information Breach and Notification Requirements

a. Contractor shall use commercially reasonable efforts to maintain the security of private information (as defined in the New York State Information Security Breach and Notification Act, as amended ("ISBNA") (General Business Law § 889-aa, § 889-bb; State Technology Law *§* 208) that it creates, receives, maintains or transmits on behalf of the University and to prevent unauthorized use and/or disclosure of that private information; and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic private information that it creates, receives, maintains or transmits on behalf of the University ("Contractor University Data"). Contractor shall disclose to the University pursuant to the ISBNA, and any other applicable law, any breach of the security of a system involving Contractor University Data following discovery or notification of the breach in the system as to any resident of New York State whose private information was, or is reasonably believed to have been acquired by a person without valid authorization ("Security Incidents"). The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Contractor shall be liable

for the costs associated with such breach if caused by the Contractor's, or that of its employees or subcontractors, negligent or willful acts or omissions, including indemnifying the University for the cost of notifying individuals, in the event of such a breach.

7. Gramm-Leach-Bliley Act

a. Pursuant to the Gramm-Leach-Bliley Act (P.L 106-102) and the Federal Trade Commission's Safeguards Rule (16 CFR Part 314) ("GLBA"), and to the extent Contractor is a financial institution or service provider of University under these regulations with respect to student or customer information, Contractor and its agents and employees will comply with the Safeguards Rule including the requirement to implement and maintain a written Information Security Program ("Program") in order to protect such nonpublic customer information (any record containing nonpublic personal information as defined in 16 CFR §313.3(n), whether in paper, electronic, or other form that is handled or maintained by or on behalf of University or its affiliates (16 CFR §314.2)) ("Nonpublic Customer Information"). Contractor shall not use, provide, trade, give away, barter, lend, sell or otherwise disclose any such Nonpublic Customer Information without University's prior written consent. If Contractor subcontracts with a third party for any of the services that it is required to undertake in accordance with the Agreement, Contractor must ensure that such third parties implement practices that protect such Nonpublic Customer Information the subcontractor receives, maintains, processes or otherwise is permitted to access in accordance with the terms of the Agreement.

8. European Union ("EU") General Data Protection Regulation ("GDPR"), People's Republic of China ("PRC") Personal Information Protection Law ("PIPL"), and other Data Privacy Laws

a. Contractor warrants any information relating to an identified or identifiable natural person ("Personal Information" or "PI") that Contractor uses, collects, retains, stores, secures, discloses, transfers, disposes of, or otherwise processes in relation to the products and services subject to the Agreement will be processed in compliance with any applicable laws, regulations, and other legal requirements relating to (a) privacy and information security; or (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of Personal Information ("PI Protection Requirements"), which may include, but is not limited to Regulation (EU) 2016/679 (the "EEA General Data Protection Regulation" or "GDPR"), and the People's Republic of China Personal Information Protection Law ("PIPL"), and Contractor shall, upon mutual agreement of the Parties, execute any amendments or addendums to the Agreement necessary for each of the Parties to maintain compliance with PI Protection Requirements. Upon request, Contractor will make available reasonable information necessary to demonstrate compliance with the obligations of any PI Protection Requirements. The Parties will cooperate in good faith to comply with PI Protection Requirements. This includes but is not limited to obtaining individuals' consent when such consent is required under PI Protection Requirements and signing and complying with all documents and agreements reasonably requested by either Party pursuant to PI Protection Requirements, including but not limited to any data processing agreements.

b. If data containing Personal Information must be transmitted by one Party to the other Party in furtherance of the activities provided for in the Agreement, both Parties agree to be responsible

for compliance with regard to such Personal Information relative to their own respective obligations in accordance with PI Protection Requirements, including but not limited to: 1) adopting and maintaining compliant privacy policies; 2) identifying a legitimate legal basis for handling the Personal Information; 3) entering into additional data handling addendum(s) as necessary to address cross-border transfer obligations under PI Protection Requirements; and 4) establishing internal organizational policies, conducting employee trainings, and engaging in regular privacy audits.

c. Contractor is, and at all prior times was, and for all times during the term of the Agreement, will remain, in material compliance with all PI Protection Requirements. To ensure compliance with the PI Protection Requirements, Contractor has in place, complies with, and takes appropriate steps reasonably designed to ensure compliance in all material respects with their policies and procedures relating to data privacy and security and the collection, storage, use, processing, disclosure, handling, and analysis of Personal Information. Contractor further certifies that neither it nor any of its Sub-Agents: (i) has received notice of any actual or potential liability under or relating to, or actual or potential violation of, any of the PI Protection Requirements, and has no knowledge of any event or condition that would reasonably be expected to result in any such notice; (ii) is currently conducting or paying for, in whole or in part, any investigation, remediation, or other corrective action pursuant to any PI Protection Requirements; or (iii) is a party to any order, decree, or agreement that imposes any obligation or liability under any PI Protection Requirements.

d. Contractor represents that it has the ability to process data on behalf of its customers in accordance with the GDPR and PIPL. If during the term of the Agreement, the Parties contemplate exchanging information that would be subject to the GDPR or PIPL, prior to sharing any such information, the Parties shall discuss in good faith a roadmap to comply with the GDPR and PIPL and shall negotiate in good faith any additional required terms and conditions (e.g., a Personal Data Processing Agreement ("DPA")).

e. Contractor warrants the Services subject to the Agreement are not subject to the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199) ("CCPA"). Following the signing of the Agreement, if any Services subject to the Agreement become subject to the CCPA, Contractor will immediately notify University and will take all actions necessary to fully comply with the CCPA, including without limitation the signing of additional data handling addendums to the Agreement.

9. Reporting and Recordkeeping

a. In addition to the reporting requirements set forth in Section 6 of this Appendix, Contractor shall, without undue delay and no later than twenty-four (24) hours of discovery, report to University any Information Security Incident. To the extent such information is known, Contractor's report shall identify at a minimum: (1) the nature of the Information Security Incident, (ii) the categories of SUNY Data involved, (iii) the causes of the Information Security Incident and possible harm caused by the Information Security Incident, (iv) what Contractor has done or shall do to mitigate any deleterious effect of the Information Security Incident, (v) what remedial measures affected individuals can adopt to mitigate harm, (vi) what corrective action Contractor

has taken or shall take to prevent future similar Information Security Incidents; and (vii) the contact information of the person or team responsible for handling the Information Security Incident. Contractor shall provide such other information, including a written report, as reasonably requested by University. Contractor shall document and retain all facts relating to an Information Security Incident and its impact, including without limitation all remedial measures taken.

10. Enforcement

a. Contractor shall be responsible for maintaining and ensuring the confidentiality and security of SUNY Data. Contractor's failure to comply with the provisions of this Appendix or that of its employees or subcontractor may result in University restricting offending individuals from access to University computer systems or SUNY Data, including Education Records, or immediately terminating the Agreement.

b. Additionally, to the extent permissible under law, the University may seek specific enforcement of Contractor's obligation of the foregoing sections, if Contractor or its employees or subcontractors breach any obligation set forth therein. In addition, Contractor shall indemnify and hold harmless the University for all damages, claims, losses, charges, and costs and expenses, including, but not limited to, counsel fees and disbursement, arising out of, related to or in connection with any such breach.