ARTICLE 1 – PURPOSE AND SCOPE OF APPLICATION

A. This Data Security and Privacy Appendix is designed to protect the University of California's (UC) Non-public Information and UC Information Resources (defined below). This Appendix describes the data security and privacy obligations of Supplier and its sub-suppliers that connect to UC Information Resources and/or gain access to Non-public Information (defined below).

B. Supplier agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Supplier also agrees to impose, by written contract, the terms and conditions contained in this Appendix on any third party retained by Supplier to provide services for or on behalf of the UC.

ARTICLE 2 – DEFINED TERMS

A. Breach. Breach means the unauthorized acquisition, access, use or disclosure of Non-public Information that compromises the security, confidentiality or integrity of such information.

B. Non-public Information. Supplier's provision of Services under this Agreement may involve access to certain information that UC wishes to be protected from further use or disclosure. Non-public Information shall be defined as: (i) Protected Information (defined below); (ii) information UC discloses, in writing, orally, or visually, to Supplier, or to which Supplier obtains access to in connection with the negotiation and performance of the Agreement, and which relates to UC, its students or employees, its third-party vendors or licensors, or any other individuals or entities that have made confidential information available to UC or to Supplier acting on UC's behalf (collectively, "UC Users"), marked or otherwise identified as proprietary and/or confidential, or that, given the nature of the information, ought reasonably to be treated as proprietary and/or confidential; (iii) trade secrets; and (iv) business information.

C. Protected Information. Protected Information shall be defined as information that identifies or is capable of identifying a specific individual, including but not limited to personally-identifiable information, medical information other than Protected Health Information as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA regulations (including, but not limited to 45 CFR § 160.103), Cardholder Data (as currently defined by the Payment Card Industry Data Security Standard and Payment Application Standard Glossary of Terms, Abbreviations, and Acronyms), student records, or individual financial information that is subject to laws restricting the use and disclosure of such information, including but not limited to Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 *et seq.*); the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); the federal Fair and Accurate Credit Transactions Act (15 USC § 1601 *et seq.*) and the Fair Credit Reporting Act (15 USC § 1681 *et seq.*).

D. UC Information Resources. UC Information Resources shall be defined as those devices, networks and related infrastructure that UC owns, operates or has obtained for use to conduct UC business. Devices include but are not limited to, UC-owned or managed storage, processing, communications devices and related infrastructure on which UC data is accessed, processed, stored, or communicated, and may include personally owned devices. Data includes, but is not limited to, Non-public Information, other UC-

created or managed business and research data, metadata, and credentials created by or issued on behalf of UC.

E. Work Product. Work Product shall be defined as works-in-progress, notes, data, reference materials, memoranda, documentation and records in any way incorporating or reflecting any Non-public Information and all proprietary rights therein, including copyrights. Work Product is subject to the Agreement's Intellectual Property, Copyright and Patents Article. For the avoidance of doubt, Work Product shall belong exclusively to UC and unless expressly provided, this Appendix shall not be construed as conferring on Supplier any patent, copyright, trademark, license right or trade secret owned or obtained by UC.

ARTICLE 3 – ACCESS TO UC INFORMATION RESOURCES

A. In any circumstance when Supplier is provided access to UC Information Resources, it is solely Supplier's responsibility to ensure that its access does not result in any access by unauthorized individuals to UC Information Resources. This includes conformance with minimum security standards in effect at the UC location(s) where access is provided. Any Supplier technology and/or systems that gain access to UC Information Resources must contain, at a minimum, the elements in the Computer System Security Requirements set forth in Attachment 1 to this Appendix. No less than annually, Supplier shall evaluate and document whether Supplier's practices accessing UC Information Resources comply with the terms of this Appendix. Documentation of such evaluation shall be made available to UC upon UC's request. Regardless of whether UC requests a copy of such evaluation, Supplier shall immediately inform UC of any findings of noncompliance and certify when findings of non-compliance have been addressed.
B. Supplier shall limit the examination of UC information to the least invasive degree of inspection required to provide the Goods and/or Services. In the event Goods and/or Services include the inspection of a specific threat to or anomaly of UC's Information Resources, Supplier shall limit such inspection in accordance with the principle of least perusal. Supplier will notify UC immediately upon such events.
C. With UC's prior written consent, Supplier may alter a UC Information Resource to the extent such alteration is specifically required for Supplier to provide Goods and/or Services to UC pursuant to the Agreement.

ARTICLE 4 – SECURITY PATCHES AND UPDATES

Supplier is required to perform patches and updates in connection with the Goods and/or Services provided to UC as follows:

A. Devices and Software Provided Directly to UC. Supplier will make available to UC any patches and other updates to system security software or firmware utilized by Supplier in its provision of Goods and/or Services no later than the earlier of thirty (30) days of its commercial release or as recommended by Supplier or Supplier's sub-supplier.
B. Supplier's Internal Systems and Services Necessary for Supplier to Fulfill its Obligations to UC. Supplier will regularly apply security patches and functional updates to its internal systems software and firmware.

ARTICLE 5 – COMPLIANCE WITH APPLICABLE LAWS, FAIR INFORMATION PRACTICE PRINCIPLES AND UC POLICIES

A. Supplier agrees to comply with all applicable state, federal and international laws, as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Protected Information. Additionally Supplier will comply as applicable with the *Fair Information Practice Principles*, as defined by the U.S. Federal Trade Commission. Such principles would typically require Supplier to have a privacy policy, and a prominently-posted privacy statement or notice in conformance with such principles. If collecting Protected Information electronically from individuals on behalf of UC, Supplier's prominently-posted privacy statement will be similar to those used by UC (UC's sample Privacy Statement for websites is available at http://www.ucop.edu/information-technology-services/policies/it-policies-and-guidelines/records-mgmt-and-privacy/files/sampleprivacystatement.doc). Supplier also agrees, to the extent applicable, to comply with UC's Business and Finance Bulletin IS-2, *Inventory, Classification, and Release of UC Electronic Information* (https://policy.ucop.edu/doc/7020447/BFB-IS-2), and IS-3, *Electronic Information Security* (https://policy.ucop.edu/doc/7000543/BFB-IS-3).
B. Supplier shall make available to UC all products, systems, and documents necessary to allow UC to audit Supplier's compliance with the terms of this Article 5. UC shall have the right to audit Supplier's compliance with its Information Security Plan and the obligations set forth in Attachment 1.
C. UC reserves the right to monitor Supplier's connectivity to UC Information Resources while Supplier accesses Non-public Information.

ARTICLE 6 – PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF NON-PUBLIC INFORMATION

Supplier agrees to hold UC's Non-public Information, and any information derived from such information, in strictest confidence. Supplier will not access, use or disclose Non-public Information other than to carry out the purposes for which UC disclosed the Non-public Information to Supplier, except as permitted or required by applicable law, or as otherwise authorized in writing by UC. For avoidance of doubt, this provision prohibits Supplier from using for its own benefit Non-public Information or any information derived from such information. If required by a court of competent jurisdiction or an administrative body to disclose Non-public Information, Supplier will notify UC in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give UC an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Supplier's transmission, transportation or storage of Non-public Information outside the United States, or access of Non-public Information from outside the United States, is prohibited except on prior written authorization by UC.

ARTICLE 7 – SAFEGUARD STANDARD

Supplier agrees to protect the privacy and security of Non-public Information according to all applicable laws and regulations, by commercially-acceptable standards, and no less rigorously than it protects its own confidential information, but in no case less than reasonable care. Supplier will implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Non-public Information. All Protected Information stored on portable devices or media must be encrypted in accordance with the Federal Information Processing Standards (FIPS) Publication 140-2. Supplier will ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Supplier has responsibility for the Non-public Information under the terms of this

Appendix. Prior to agreeing to the terms of this Appendix, and periodically thereafter (no more frequently than annually) at UC's request, Supplier will provide assurance, in the form of a third-party audit report or other documentation acceptable to UC, such as SOC2 Type II, demonstrating that appropriate information security safeguards and controls are in place.

ARTICLE 8 – INFORMATION SECURITY PLAN

A. Supplier acknowledges that UC is required to comply with information security standards for the protection of Protected Information as required by law, regulation and regulatory guidance, as well as UC's internal security program for information and systems protection.

B. Supplier will establish, maintain and comply with an information security plan ("Information Security Plan"), which will contain, at a minimum, such elements as those set forth in Attachment 1 to this Appendix.

C. Supplier's Information Security Plan will be designed to:
   i. Ensure the security, integrity and confidentiality of Non-public Information;
   ii. Protect against any anticipated threats or hazards to the security or integrity of such information;
   iii. Protect against unauthorized access to or use of such information that could result in harm or inconvenience to the person that is the subject of such information;
   iv. Reduce risks associated with Supplier having access to UC Information Resources; and
   v. Comply with all applicable legal and regulatory requirements for data protection.

D. On at least an annual basis, Supplier will review its Information Security Plan, update and revise it as needed, and submit it to UC upon request. At UC's request, Supplier will make modifications to its Information Security Plan or to the procedures and practices thereunder to conform to UC's security requirements as they exist from time to time. If there are any significant modifications to Supplier's Information Security Plan, Supplier will notify UC within 72 hours.

ARTICLE 9 – RETURN OR DESTRUCTION OF NON-PUBLIC INFORMATION

Within 30 days of the termination, cancellation, expiration or other conclusion of this Appendix, Supplier will return the Non-public Information to UC unless UC requests in writing that such data be destroyed. This provision will also apply to all Non-public Information that is in the possession of subcontractors or agents of Supplier. Such destruction will be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Supplier will certify in writing to UC that such return or destruction has been completed.

If Supplier believes that return or destruction of the Non-public Information is technically impossible or impractical, Supplier must provide UC with a written statement of the reason that return or destruction by Supplier is technically impossible or impractical. If UC determines that return or destruction is technically impossible or impractical, Supplier will continue to protect the Non-public Information in accordance with the terms of this Appendix.

ARTICLE 10 – NOTIFICATION OF CORRESPONDENCE CONCERNING NON-PUBLIC INFORMATION

Supplier agrees to notify UC immediately, both orally and in writing, but in no event more than two (2) business days after Supplier receives correspondence or a complaint regarding Non-public Information, including but not limited to, correspondence or a complaint that originates from a regulatory agency or an individual.

ARTICLE 11 – BREACHES OF NON-PUBLIC INFORMATION

A. **Reporting of Breach**: Supplier will report any confirmed or suspected Breach to UC immediately upon discovery, both orally and in writing, but in no event more than two (2) business days after Supplier reasonably believes a Breach has or may have occurred. Supplier's report will identify: (i) the nature of the unauthorized access, use or disclosure, (ii) the Non-public Information accessed, used or disclosed, (iii) the person(s) who accessed, used, disclosed and/or received Non-public Information (if known), (iv) what Supplier has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action Supplier has taken or will take to prevent future unauthorized access, use or disclosure. Supplier will provide such other information, including a written report, as reasonably requested by UC. In the event of a suspected Breach, Supplier will keep UC informed regularly of the progress of its investigation until the uncertainty is resolved.

B. **Coordination of Breach Response Activities:** Supplier will fully cooperate with UC's investigation of any Breach involving Supplier and/or the Services, including but not limited to making witnesses and documents available immediately upon Supplier's reporting of the Breach. Supplier's full cooperation will include but not be limited to Supplier:
   i. Immediately preserving any potential forensic evidence relating to the Breach, and remedying the Breach as quickly as circumstances permit
   ii. Promptly (within 2 business days) designating a contact person to whom UC will direct inquiries, and who will communicate Supplier responses to UC inquiries;
   iii. As rapidly as circumstances permit, applying appropriate resources to remedy the Breach condition, investigate, document, restore UC service(s) as directed by UC, and undertake appropriate response activities;
   iv. Providing status reports to UC on Breach response activities, either on a daily basis or a frequency approved by UC;
   v. Coordinating all media, law enforcement, or other Breach notifications with UC in advance of such notification(s), unless expressly prohibited by law; and
   vi. Ensuring that knowledgeable Supplier staff is available on short notice, if needed, to participate in UC-initiated meetings and/or conference calls regarding the Breach.

C. **Grounds for Termination.** Any Breach may be grounds for immediate termination of the Agreement by UC.

D. **Assistance in Litigation or Administrative Proceedings.** Supplier will make itself and any employees, subcontractors, or agents assisting Supplier in the performance of its obligations available to UC at no cost to UC to testify as witnesses, or otherwise, in the event of a Breach or other unauthorized disclosure of Non-public Information caused by Supplier that results in litigation, governmental investigations, or administrative proceedings against UC, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy or arising out of this Appendix.

ARTICLE 12 – ATTORNEY'S FEES

In any action brought by a party to enforce the terms of this Appendix, the prevailing party will be entitled to reasonable attorney's fees and costs, including the reasonable value of any services provided by in-house counsel. The reasonable value of services provided by in-house counsel will be calculated by applying an hourly rate commensurate with prevailing market rates charged by attorneys in private practice for such services.

ARTICLE 13 – INDEMNITY

The Agreement includes an Indemnity provision, but for the avoidance of doubt regarding a Breach involving Protected Information, Supplier's indemnification obligations under the Agreement will include the following fees and costs which arise as a result of Supplier's breach of this Appendix, negligent acts or omissions, or willful misconduct: any and all costs associated with notification to individuals or remedial measures offered to individuals, whether or not required by law, including but not limited to costs of notification of individuals, establishment and operation of call center(s), credit monitoring and/or identity restoration services; time of UC personnel responding to Breach; fees and costs incurred in litigation; the cost of external investigations; civil or criminal penalties levied against UC; civil judgments entered against UC; attorney's fees, and court costs.

ARTICLE 14 – ADDITIONAL INSURANCE

In addition to the insurance required under the Agreement, Supplier at its sole cost and expense will obtain, keep in force, and maintain an insurance policy (or policies) that provides coverage for privacy and data security breaches. This specific type of insurance is typically referred to as Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability. In some cases, Professional Liability policies may include some coverage for privacy and/or data breaches. Regardless of the type of policy in place, it needs to include coverage for reasonable costs in investigating and responding to privacy and/or data breaches with the following minimum limits unless UC specifies otherwise: $1,000,000 Each Occurrence and $5,000,000 Aggregate.

FIRST AMENDMENT TO APPENDIX – DATA SECURITY AND PRIVACY
SAFEGUARD STANDARD FOR PAYMENT CARD DATA (IF APPLICABLE)

A. Supplier agrees that it is responsible for the security of Cardholder Data (as currently defined by the Payment Card Industry Data Security Standard and Payment Application Standard Glossary of Terms, Abbreviations, and Acronyms) that it possesses (if any), including the functions relating to storing, processing and transmitting Cardholder Data. In this regard, Supplier represents and warrants that it will implement and maintain certification of Payment Card Industry ("PCI") compliance standards regarding data security, and that it will undergo independent third party quarterly system scans that audit for all known methods hackers use to access private information and vulnerabilities that would allow malicious software (*e.g.*, viruses and worms) to gain access to or disrupt UC Information Resources. These requirements, which are incorporated herein, can be found at https://www.pcisecuritystandards.org/document_library. Supplier agrees to provide at least annually, and from time to time at the written request of UC, current evidence (in form and substance reasonably satisfactory to UC) of compliance with these data security standards, which has been properly certified by an authority recognized by the payment card industry for that purpose.

B. In connection with credit card transactions processed for UC, Supplier will provide reasonable care and efforts to detect fraudulent payment card activity. In performing the Services, Supplier will comply with all applicable rules and requirements, including security rules and requirements, of UC's financial institutions, including its acquiring bank, the major payment card associations and payment card companies. If during the term of an Agreement with UC, Supplier undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI standards and/or other material payment card industry standards, it will promptly notify UC of such circumstances.

C. Supplier further represents and warrants that software applications it provides for the purpose of performing Services related to processing payments, particularly credit card payments, are developed in accordance with all applicable PCI standards, and are in compliance with all applicable PCI standards, including but not limited to Payment Application Data Security Standards (PA-DSS), Point to Point Encryption Solution Requirements (P2PE) including approved card readers or Point of Interaction (POI). As verification of this, Supplier agrees to provide at least annually, and from time to time upon written request of UC, current evidence (in form and substance reasonably satisfactory to UC) that any such application it provides is certified as complying with these standards and agrees to continue to maintain that certification as may be required.

D. Supplier will immediately notify UC if it learns that it is no longer PCI compliant under one of the standards identified above, or if any software applications or encryption solutions are no longer PCI compliant.

ATTACHMENT 1

A. Supplier will develop, implement, and maintain a comprehensive Information Security Plan that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards. The safeguards contained in such program must be consistent with the safeguards for protection of Protected Information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

B. Without limiting the generality of the foregoing, every comprehensive Information Security Plan will include, but not be limited to:

   i. Designating one or more employees to maintain the comprehensive Information Security Plan;

   ii. Identifying and assessing internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information and of UC Information Resources, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
      a. Ongoing employee (including temporary and contract employee) training;
      b. Employee compliance with policies and procedures; and
      c. Means for detecting and preventing security system failures.

   iii. Developing security policies for employees relating to the storage, access and transportation of records containing Protected Information outside of business premises.

   iv. Imposing disciplinary measures for violations of the comprehensive Information Security Plan rules.

   v. Preventing terminated employees from accessing records containing Protected Information and/or UC Information Resources.

   vi. Overseeing service providers, by:
      a. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such Protected Information and UC Information Resources consistent with all applicable laws and regulations; and
      b. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for Protected Information.

   vii. Placing reasonable restrictions upon physical access to records containing Protected Information and UC Information Resources and requiring storage of such records and data in locked facilities, storage areas or containers.

   viii. Restrict physical access to any network or data centers that may have access to Protected Information or UC Information Resources.

ix. Requiring regular monitoring to ensure that the comprehensive Information Security Plan is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Protected Information and UC Information Resources; and upgrading information safeguards as necessary to limit risks.

x. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Protected Information and of UC Information Resources.

xi. Documenting responsive actions taken in connection with any incident involving a Breach, and mandating post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Protected Information and UC Information Resources.

Computer System Security Requirements

To the extent that Supplier electronically stores or transmits Protected Information or has access to any UC Information Resources, it will include in its written, comprehensive Information Security Plan the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, will have the following elements:

A. Secure user authentication protocols including:
   i. Control of user IDs and other identifiers;
   ii. A secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
   iii. Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
   iv. Restricting access to active users and active user accounts only; and
   v. Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
   vi. Periodic review of user access, access rights and audit of user accounts.

B. Secure access control measures that:
   i. Restrict access to records and files containing Protected Information and systems that may have access to UC Information Resources to those who need such information to perform their job duties; and
   ii. Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, which are reasonably designed to maintain the integrity of the security of the access controls.

C. Encryption of all transmitted records and files containing Protected Information.

D. Adequate security of all networks that connect to UC Information Resources or access Protected Information, including wireless networks.

E. Reasonable monitoring of systems, for unauthorized use of or access to Protected Information and UC Information Resources.

F. Encryption of all Protected Information stored on Supplier devices, including laptops or other portable storage devices.

G. For files containing Protected Information on a system that is connected to the Internet or that may have access to UC Information Resources, reasonably up-to-date firewall, router and switch protection and operating system security patches, reasonably designed to maintain the integrity of the Protected Information.

H. Reasonably up-to-date versions of system security agent software, including intrusion detection systems, which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

I. Education and training of employees on the proper use of the computer security system and the importance of Protected Information and network security.

With reasonable notice to Supplier, UC may require additional security measures which may be identified in additional guidance, contracts, communications or requirements.

FIRST AMENDMENT TO APPENDIX – DATA SECURITY AND PRIVACY
GENERAL DATA PROTECTION REGULATION DATA PROTECTION AMENDMENT

During the course of providing Services to, or on behalf of, UC pursuant to the Agreement between UC and Supplier dated _____, Supplier may access or otherwise process personal data as defined below. The Parties agree that with respect to the processing of personal data pursuant to the Agreement or this Data Protection Amendment ("DPA"), UC is the data controller (and shall hereinafter be referred to as the "Controller"), and Supplier is the data processor (and shall hereinafter be referred to as the "Processor"). The Parties have agreed that the Processor will provide the Services to the Controller pursuant to and in accordance with the terms and conditions of the Agreement and this DPA. In the event of a conflict between the terms of this DPA and the Agreement, the terms of this DPA shall govern. Supplier agrees to be bound by the obligations set forth in this DPA. To the extent applicable, Supplier also agrees to impose, by written contract, the terms and conditions contained in this DPA on any third party retained by Supplier to provide services for or on behalf of UC.

A. Definitions

Capitalized terms used but not defined in this DPA will have the meanings set forth in the Agreement. The following capitalized terms shall have the meanings set forth herein:

1. "**Data**" means all personal data processed by (or on behalf of) the Processor for the Controller under or in connection with the Agreement, including in the provision of the Services. "Data" as used herein shall also be considered UC Protected Information as defined in Appendix DS;

2. "**Data Subjects' Rights**" means the rights of data subjects as provided in the GDPR including, but not limited to, rights of access, rectification, erasure, restriction of processing, data portability, objection, and the right not to be subject to automated decision making (including profiling);

3. "**EEA**" means European Economic Area;

4. "**EU**" means the European Union;

5. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

6. "**data subject**," "**personal data**," "**personal data breach**," "**process/processing**," "**pseudonymisation**," and "**supervisory authority**," shall each have the meaning as in the GDPR;

7. "**Subprocessor**" means any third party: (i) who is engaged by the Processor to carry out specific processing activities relating to Data for or on behalf of the Controller; or (ii) to whom the Processor subcontracts any of its obligations in connection with the Agreement.

B. Scope of Processing Data

1. Processor shall process Data solely for the purposes of performing the Services and for the same duration of the Agreement, except as otherwise agreed to in writing by the Parties. The scope and

further details of Processor's processing activities of Data pursuant to the Agreement DPA are set forth in Addendum A to this DPA.

2. To the extent any additional information is required to be included in the Addendum pursuant to the GDPR or any other applicable EU Member State or EEA state law, or this Agreement otherwise requires amendment, the Parties will cooperate to amend this DPA in a writing signed by both Parties.

C. Subprocessors

1. Except as otherwise set forth in the Addendum, the Processor shall not engage any Subprocessor, or subcontract any of its obligations under or in connection with the Agreement to any Subprocessor, without the prior specific written consent of the Controller.

2. If the Controller approves of any Subprocessor pursuant to the Addendum, the Processor shall give the Controller prior written notice of any intended changes concerning the addition or replacement of such Subprocessors to allow the Controller to approve or object to such changes. Such notice shall include details of the processing activity or activities to be conducted by the applicable Subprocessor and the identity and contact details of such Subprocessor.

3. The Processor shall ensure that any Subprocessor approved by Controller in accordance with this Section C is subject to obligations in a written agreement requiring such Subprocessor to comply with the obligations of this DPA, including, but not limited to, providing sufficient guarantees to implement appropriate technical and organizational measures as required by GDPR. If any Subprocessor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the performance or non-performance of such Subprocessor.

4. Upon request, the Processor shall provide a copy of each Subprocessor agreement entered into pursuant to this Section C to the Controller.

D. Obligations of the Processor

1. The Processor shall, and shall ensure that each of its employees, approved Subprocessors and any other individual acting under its authority who has access to the Data shall:

   a. process Data in accordance with the terms of this Agreement, DPA or any other written instructions of the Controller, and only to the extent and in the manner necessary to provide Services, and for no other purpose(s). In the event EU or Member State law requires Processor to process in a manner not expressly authorized by this Agreement or the Controller's written instructions, the Processor shall promptly inform the Controller of the applicable legal requirement before processing, unless prohibited from doing so on important public interest grounds, consistent with EU or Member State law;

   b. keep the Data confidential and ensure that any person authorized to process the Data for or on behalf of the Processor (including but not limited to any Processor employees and staff and approved Subprocessors) has agreed to keep the Data confidential, or is otherwise under a statutory obligation to protect the confidentiality of the Data; and

c. upon reasonable request from the Controller, provide an up-to-date copy of the Data in the format requested by the Controller.

2. In carrying out its obligations under the Agreement and this DPA, the Processor shall comply with all applicable laws and regulations relating to privacy or data protection, including, but not limited to, GDPR.

3. In accordance with GDPR, and taking into consideration the state of the art, costs of implementation and the nature, scope, context and purposes of processing the Data pursuant to this Agreement, as well as the risks to the rights and freedoms of natural persons and the risks to processing the Data, the Processor represents and warrants that it shall implement appropriate technical and organizational security measures appropriate to such risks, including, as appropriate: (i) the pseudonymisation and encryption of the Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability of and access to the Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

4. The Processor's technical and organizational security measures to protect Data shall include, without limitation, the measures set forth in Appendix DS.

5. The Processor shall assist the Controller in ensuring compliance with Controller's obligations as a Controller by: (a) cooperating with Controller's implementation of appropriate technical and organizational security measures to ensure the security of processing Data; (b) cooperating with Controller notifications to supervisory authorities and/or data subjects, as applicable, of any breaches of Data; (c) cooperating with Controller's conduct of data protection impact assessments, including but not limited to, any requirements to consult with a supervisory authority as required by GDPR. Processor shall also cooperate with additional obligations of Controller that may be required of it pursuant to GDPR and other applicable data protection laws.

6. In the event of any suspected or actual personal data breach, the Processor shall notify the Controller (via the individual identified by UC in the Agreement to receive Notices relating to Appendix DS on behalf of UC) orally and in writing (including by e-mail) immediately after becoming aware of such breach. All breach reporting of Data shall otherwise be consistent with Article 11 of Appendix DS.

7. Except for transfers of Data to the Controller, the Processor shall not process or transfer any Data to any country outside the EEA except pursuant to prior written approval of the Controller, and at all times in compliance with GDPR and other applicable data protection laws.

8. This section is only applicable if Processor's Services include the collection of personal data directly from data subjects: In the event Processor's Services include the collection of personal data directly from data subjects that is to be provided to Controller, unless the parties otherwise agree, the Processor shall be responsible for ensuring that such processing of personal data complies with GDPR requirements, including, but not limited to, obtaining a lawful basis to process the personal data.

9. This section is only applicable if Processor's Services include the transfer of personal data it has collected or obtained from the EEA to Controller: In the event Processor is transferring personal data it has

collected or otherwise obtained from data subjects in the EEA to Controller for the purposes of performing Services, unless the parties otherwise agree on another transfer mechanism which satisfies GDPR requirements, such transfers shall be governed by the Standard Contractual Clauses set forth in Addendum B to this DPA. Processor acknowledges that Controller is subject to U.S. federal and state laws and regulations, including but not limited to public disclosure laws and regulations that may require the retention and disclosure of information that is the subject of the Agreement. Any liability, claims or damages of Controller shall be limited to the acts or omissions of the Controller. Processor acknowledges that Controller is a U.S. state public institution and is prohibited from assuming liability for the conduct of persons other than Controller's officers, agents, employees, students, invitees, and/or guests.

10. The Processor shall return or destroy Data consistent with the provisions of Article 9 of Appendix DS. In the event EU, EU Member State law or EEA state law requires the storage of such Data, the Processor shall promptly inform the Controller of such requirement.

E. <u>Data Subjects' Rights</u>

1. Except as otherwise set forth in writing by Controller, the Controller shall be responsible for providing data subjects with any information required under GDPR at the time of collecting such data subjects' personal data, as well as any information requested by data subjects relating to the processing of their personal data.

2. The Processor shall notify the Controller (via the individual identified by UC in the Agreement to receive Notices relating to Appendix DS on behalf of UC) in writing (including by e-mail) of each and any request that it receives from a data subject relating to a Data Subject Right. Such written notification shall be made promptly no later than two (2) business days following receipt of the request, and shall include any information in the Processor's custody or control that may assist the Controller to respond to the request.

3. Unless otherwise required by applicable EU, EU Member State law or EEA state law, the Processor shall not respond to any such requests or other communications the Processor receives from data subjects, without the prior written consent of the Controller.

4. The Processor shall assist the Controller in Controller's obligations to respond to requests for exercising Data Subjects' Rights by using appropriate technical and organizational measures, to the extent practicable given the nature of the processing of Data.

F. <u>Accountability</u>

1. Upon written request from the Controller, the Processor shall make available to the Controller all information necessary to demonstrate compliance with its obligations under this DPA. The Processor shall make its records, documents, facilities, processes and individuals reasonably available to Controller or Controller's designee for audits or inspections to demonstrate compliance with this DPA.

2. The Processor shall immediately inform the Controller if, in the Processor's opinion, any instruction from the Controller with respect to the processing of Data pursuant to this Agreement violates or contradicts GDPR, or other applicable EU, EU Member State or EEA state data protection laws or regulations.

Addendum A: Scope of Processing Data

This Addendum is part of the DPA and includes details of the processing of Data as required by the Agreement.

1. Processor is processing Data on behalf of the Controller for purposes of the performance of Services described in this Agreement. Data shall be processed for the duration of the term of this Agreement, except as otherwise specifically set forth herein. [IF THE DATA WILL BE PROCESSED BY THE PROCESSOR FOR PURPOSES OF PROVIDING SERVICES BEYOND THE DURATION OF THE TERM OF THE AGREEMENT, DESCRIBE THAT HERE.]

2. The purposes(s) of the processing of Data to be carried out by the Processor on behalf of the Controller includes: [e.g., administration of payroll to employees; quality improvement of laboratory testing]

3. The Data to be processed by the Processor on behalf of the Controller in the performance of Services includes the following: [BUYER TO IDENTIFY TYPES OF DATA, E.G., NAME, TITLE, CONTACT INFORMATION, BIRTHDATE, AGE, IDENTIFICATION NUMBERS, ACADEMIC RECORDS, FINANCIAL DATA,] [Insert, if applicable: the Data also includes the following sensitive data – [choose as appropriate]: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation, or data relating to criminal convictions or offenses] If the Processor becomes aware that additional personal data and/or UC Protected Information not identified above has been received from the Controller, the Processor shall immediately notify the Controller.

4. The Data to be processed by the Processor on behalf of the Controller in the performance of Services relates to the following categories of data subjects: [E.G., PATIENTS, STUDENTS, DONORS, EMPLOYEES, VENDORS, CONSULTANTS.]

5. [Insert if applicable: Controller authorizes the Processor to subcontract the following processing activities to the following Subprocessors: [insert the name and contact information of each Subprocessor, and a description of the type of processing activities the Subprocessor will conduct.]

6. [Insert if applicable: Other than to the United States as may be required for the performance of Services, and for which the Controller has a lawful basis to transfer the Data to the United States pursuant to GDPR, the Processor may transfer Data to the following countries outside of the EEA: [insert information relating to the country, recipient, and details regarding how the transfer will be in compliance with GDPR. Consult OGC for guidance if the Processor requires inclusion of this Section.]]