CALIFORNIA STATE UNIVERSITY DATA PRIVACY AND SECURITY RIDER

Contract Number:

This Data Privacy and Security Rider ("DPS Rider") is made part of that certain Contract for Purchase of Goods, Software, or Services with the contract number written above ("Contract"), made by and between the contractor named in such Contract ("Contractor") and The Trustees of the California State University ("CSU" or "University"). CSU and Contractor are individually referred to herein as a "Party", and together referred to as the "Parties". This DPS Rider supplements the California State University Terms and Conditions of Purchase.

The Parties agree that the following terms and conditions are incorporated into the Contract:

1. **Definitions.** For purposes of this Contract:
   a. Terms that are capitalized in this Rider shall have the same meanings as those terms are defined in the California State University Terms and Conditions of Purchase.
   b. "Representative" shall mean an employee (full time or part time), officer, director, or agent of a Party.
   c. "Affiliate" shall mean an entity now or hereafter controlled by, controlling or under common control with a Party; control exists when an entity owns or controls more than 50% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity.
   d. "Subcontractor" shall mean a third party to whom Contractor has delegated or subcontracted any portion of its obligations set forth herein.

2. **University Data.** Under the Contract, Contractor will do one or more of the following: create, obtain, access, transmit, maintain, use, process, store, host, or dispose of University Data.

3. **Personnel Security Requirements.**
   a. **Need to Know**. Contractor shall permit access to University Data only to those Representatives, Affiliates, or Subcontractors of Contractor who require such access to carry out the purposes of this Contract.
   b. **Security Training.** Contractor shall require all Representatives, Affiliates and Subcontractors with access to University Data, as a condition of their engagement, to participate in annual security awareness training.
   c. **Record Access.** Contractor shall not knowingly permit a Representative, Affiliate, or Subcontractor to have access to the records, data or premises of CSU when such Representative, Affiliate or Subcontractor:
      (a) has been convicted of a crime;
      (b) has engaged in a dishonest act or a breach of trust; or
      (c) uses illegal drugs.
   d. **Personal Devices.** At no time shall Contractor's Representatives, Affiliates or Subcontractors connect to any CSU system or access any University Data, for purposes of downloading, extracting, storing or transmitting data, using personally owned, rented or borrowed equipment, including but not limited to mobile devices.
   e. **Background Checks.** Contractor shall maintain comprehensive hiring policies and procedures which include, among other things, a background check for criminal convictions, and pre-employment drug testing, to the extent permitted by law. Contractor shall conduct background checks and obtain references for all its Representatives, Affiliates, and Subcontractors who have access to University Data. Such background checks shall include but not be limited to: Social Security Number trace; seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for criminal convictions CSU deems inconsistent with

assigned duties; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC).

f. **Contract Flow-Down.** Contractor shall require all its Affiliates and Subcontractors, as a condition to their engagement, to agree to be bound by provisions substantially similar to those included in this Contract related to information security matters.

g. **Subcontractors.** Contractor shall notify University, on a continuing basis, of all subcontractors which may have access to University Data.

4. **Information Security Plan.** Contractor shall develop, implement, maintain and use appropriate administrative, technical and physical security measures, which may include but not be limited to encryption techniques, to preserve the confidentiality, integrity and availability of all University Data. No later than 30 days after the Effective Date of this Contract, and subject to the review and approval of CSU, Contractor shall establish, maintain, comply with, and provide to CSU an information security plan ("Information Security Plan"), which shall:

i. ensure the security, integrity and confidentiality of University Data;
ii. protect against any anticipated threats or hazards to the security or integrity of University Data;
iii. protect against unauthorized access to or use of University Data that could result in substantial harm or inconvenience to the person that is the subject of University Data;
iv. protect against unauthorized changes to or use of University Data;
v. comply with all applicable CSU policies legal and regulatory requirements for data protection;
vi. include business continuity and disaster recovery plans; and
vii. include a written response program addressing the appropriate remedial measures it shall undertake in the event that there is a Security Incident.

Contractor shall cause all Subcontractors and other persons and entities whose services are part of the Contracted Work or who hold University Data, to implement an information security program and plan substantially equivalent to Contractor's. The Information Security Plan shall require that any Level 1 – Confidential data transmitted or stored by Contractor only be transmitted or stored in an encrypted form acceptable to CSU.

If requested by CSU, on at least an annual basis, Contractor shall review, update and revise its Information Security Plan, subject to CSU's review and approval. At CSU's request, Contractor shall make modifications to its Information Security Plan or to the procedures and practices thereunder to conform to CSU's security requirements as they exist from time to time.

5. **Risk Assessments.**

a. **Self-Assessment.** Contractor shall conduct risk assessments and/or audits of its use of University Data at least annually. Upon request by CSU, Contractor shall provide CSU with copies of its latest information security risk assessments and/or audits. If any assessment and/or audit discloses material variances from the performance requirements set forth in this Contract, Contractor shall be deemed in breach of this Contract.

b. **SOC Report.** Upon request by CSU, Contractor shall provide to CSU, at no cost, its most recent AICPA Service Organization Control (SOC 2 Type 2) audit report and that of all subservice provider(s) relevant to the Contract. If so requested by CSU, such SOC report shall be provided annually, within 30 days of its issuance by the auditor, and shall be directed to the appropriate representative identified by CSU. Contractor shall provide CSU with a designated point of contact for the SOC report, address issues raised in the SOC report with relevant subservice provider(s), and respond to any follow-up questions posed by CSU in relation to the SOC report.

c. **Audit by CSU.** During regular business hours, CSU may, at its sole expense and on a mutually agreed upon date (which shall be no more than fourteen (14) days after written notice), time, location and duration, perform or arrange for a site visit and/or confidential audit of Contractor's operations, facilities, financial records, and security and business continuity systems which pertain specifically to the Contracted Work. If Contractor is not in substantial compliance with the requirements of the performance requirements set forth in this Contract, CSU shall be entitled, at Contractor's expense, to perform additional such assessments and/or audits. CSU will provide to Contractor a copy of each report prepared in connection with any such audit within thirty (30) calendar days after it prepares or receives such report. Contractor agrees to promptly take action at its expense to correct those matters or items that require correction.

d. **Default**. If any assessment and/or audit discloses material variances from the performance requirements or terms of this Contract, Contractor shall be deemed in breach of this Contract.

6. **Data Encryption.** Contractor warrants that all electronic data will be encrypted in transmission (including via web interface) and stored at no less than 256-bit level encryption. Contractor warrants that all University Data shall be securely destroyed, when destruction is requested by CSU.

7. **Network Security.** Contractor agrees to maintain network security that, at a minimum conforms to one of the following:
   i. Current standards set forth and maintained by the National Institute of Standards and Technology, as found at https://nvd.nist.gov; or
   ii. Any generally recognized, comparable standard that Contractor then applies to its own network (*e.g.* ISO 27002) and which has been approved in writing by CSU.

8. **Security Code Access.** Contractor will be responsible for safekeeping all keys, access codes, combinations, access cards, personal identifying numbers and similar security codes, identifiers, passwords or authenticators issued to Contractor's employees, agents, contractors or subcontractors working with CSU accounts. Contractor agrees to report a lost or stolen device or information of these employees within 24 hours of such device or information being lost or stolen.

9. **Assistance with eDiscovery**. Contractor will make itself and any Representatives, Affiliates, Subcontractors, and/or agents assisting in the performance of its obligations under the Agreement, available to CSU at no cost to CSU. This shall include, without limitation, any data preservation or eDiscovery required by CSU or testimony, or otherwise, in the event of litigation or administrative proceeding.

10. **Supplemental Provisions.** The following subsections are incorporated in the Contract only if the box preceding that subsection is checked:

☐ a. **HIPAA.** Contractor provides Goods or Services which involves patient health information under HIPAA. Contractor shall use and disclose Protected Health Information in compliance with the security standards for the protection of electronic protected health information provided in 45 C.F.R. Parts 160 and 164.

☐ b. **Records Retention.** Contractor provides a product or Service which involves storage of CSU records. Contractor shall maintain all records pertaining to the Contracted Work for the periods of time required by the CSU Retention schedule (at https://www.calstate.edu/recordsretention), including following termination of this Contract, subject to applicable law or regulation. Contractor further agrees to provide to CSU, at its request, a full copy of all such records for CSU to maintain at a U.S. location designated by CSU. Destruction or deletion of data shall be in accordance with the most current version of ISO 27001. Contractor shall provide evidence or certification that this section has been complied with.

☐ c. **PCI Compliance Standards.** Contractor provides a service that involve storage, processing or transmission of payment card data. Contractor represents and warrants that it shall implement and maintain certification of Payment Card Industry ("PCI") compliance standards regarding data security and that it shall undergo independent third-party quarterly system scans that audit for all known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e., viruses and worms) to gain access to or disrupt the network devices. If during the term of the Agreement, Contractor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI DSS standards and/or other material payment card industry standards, it will promptly notify CSU of such circumstances.

Contractor agrees to promptly provide current evidence of compliance with PCI-DSS standards at CSU's request and on an annual basis thereafter. The form and substance of such evidence must be reasonably satisfactory to and must be certified by an authority recognized by the payment card industry for that purpose. Contractor shall maintain and protect in accordance with all applicable laws and PCI regulations the security of all cardholder data when performing the contracted Services on behalf of CSU. Contractor will provide reasonable care and efforts to detect fraudulent credit card activity in connection with credit card transactions processed for CSU. Contractor shall indemnify and hold CSU harmless from loss or damages resulting from Contractor's failure to maintain PCI compliance standard in accordance with this section. Contractor shall not be held responsible for any such loss of data if it is shown that the loss occurred as a result of the sole negligence of CSU.

☐ d. **ACH Transaction Compliance.** Contractor provides Goods or Services which involves ACH payments. Contractor agrees to assist CSU in documenting compliance with NACHA rules and regulations and with compliance of security standards for the protection of ACH transactions.