OpenAI Services Agreement

Customer Name	Trustees of the California State University
Customer Address	401 Golden Shore Long Beach CA 90802
Customer Notices Address	California State University, Office of the Chancellor Contract Services & Procurement Attn: Laura Bennett 401 Golden Shore Long Beach CA 90802 lbennett@calstate.edu (562)951-4974 If blank, same as above.
Effective Date	Date last signed by a Party below.

This OpenAI Services Agreement ("Agreement") is entered as of the Effective Date between the customer identified above ("Customer") and OpenAI, LLC, unless Customer is based within a European Economic Area country or Switzerland, in which case it is entered into with OpenAI Ireland Ltd. ("OpenAI"). For the first sixty (60) days following the Effective Date, the parties agree to collaborate in good faith on any additional or supplemental terms that Customer needs to add to this Agreement. Capitalized terms not defined in the Agreement have the meanings provided in the Order Form. In this Agreement, OpenAI and Customer are each referred to as a "Party" and collectively as the "Parties." This Agreement is accepted and agreed to by the authorized representative of each Party:

OpenAI:	**Customer: Trustees of the California State University**
Signature: Aliisa Rosenthal Aliisa Rosenthal (Jan 17, 2025 16:41 PST)	Signature: David Beaver
Name: Aliisa Rosenthal	Name: David Beaver
Title: Head of Enterprise	Title: Chief Procurement Officer
Date: Jan 17, 2025	Date: Jan 17, 2025

1. Services.

1.1. Services Term. OpenAI will deliver the Services to Customer for the Services Term. The Services Term will be listed on the Order Form. Unless the Parties agree otherwise in writing, increases in the Services purchased during a Services Term will have a prorated term ending concurrently with the then-current Services Term. OpenAI will not commence work under this Agreement until it is fully executed between the parties; any work performed by OpenAI prior to that date is performed at OpenAI's risk and as a volunteer.

1.2. Renewal. Renewal Terms, if any, and whether the Services auto renew, will be listed on the applicable Order Form. Notice of non-renewal or scope reduction must be given at least thirty days before the start of the next Renewal Term.

1.3. Authorized Purchasers.

a. Provisioning. To provision the Services, OpenAI requires the email address of the initial Authorized Purchaser to be included on the Order Form. Failure to include correct Authorized Purchaser information on the Order Form may result in delays.

b. Purchases. The Services may be configured to allow Authorized Purchasers to purchase additional licenses,

quantities, or volumes of Services. Customer is responsible for understanding the Services settings that allow additional purchases. OpenAI will charge Customer for additional licenses, quantities, or volumes of Services for the remainder of the then-current Services Term based on Customer's then-current price unless otherwise set forth on the Order Form.

1.4. Affiliates.

1. Usage. OpenAI provisions the Services to specific entities using dedicated workspaces and organizational IDs. Customer Affiliates may purchase and use the Services under Customer's Account, which means Customer and its Affiliates usage will occur in the same workspace and under the same organizational ID.

2. Separate Purchases. If Customer Affiliates' purchase and use of the Services is intended to be separate from Customer's, then Customer or its Affiliate must execute a separate Order Form. OpenAI will then create a separate workspace and organizational ID for that Affiliate and provision the Services accordingly. If Customer Affiliates enter into Order Forms under this Agreement they will be bound by this Agreement. Customer will be responsible and liable for all acts and omissions of its Affiliates that access the Services under this Agreement.

1.5. Usage-based Services. If Customer purchases Services based on usage, Customer acknowledges that OpenAI will charge Customer the Fees for the Services based on the usage calculated by OpenAI.

2. Provision.

2.1. General. The Agreement governs Customer's access to and use of the Services. Customer may access and use the Services in accordance with the Agreement. All prior agreements, representations, inducements, and negotiations, and any and all existing contracts previously executed between the parties with respect to this subject matter, are superseded hereby. This Contract also supersedes all click-through, click-wrap, shrink-wrap, Terms of Use, Terms of Service, or other End User License Agreements, all of which are null and void. CSU rejects any different or additional terms without prior written consent from an authorized CSU officer or employee.

2.2. OpenAI will provide the Services as an independent contractor and will devote industry standard qualified personnel to perform any applicable Services under the Agreement. At no time will OpenAI or OpenAI's employees or personnel be considered employees of Customer for any purpose, including but not limited to workers' compensation provisions.

2.3. Use. OpenAI grants Customer a non-exclusive right to access and use the Services during the Term. This includes the right to use OpenAI's API to integrate the Services into Customer Applications and to make Customer Applications available to End Users. OpenAI will not use any Customer Content, including but not limited to audio, video, text, screen sharing, attachments, (Customer Input) or ChatGPT Output, to train OpenAI or third-party artificial intelligence models. OpenAI is responsible to Customer for all Services performed by OpenAI's employees, agents or subcontractors under this Agreement, including responsibility for ensuring payment of any unemployment, social security, payroll, contributions or other taxes with respect to such employees, agents and subcontractors.

2.4. Modifications. OpenAI may update the Services periodically. At no time will Customer's access, feature-set or functionality permanently degrade below those available to ChatGPT Education customers. If an OpenAI update materially reduces the Services functionality, OpenAI will notify Customer at the Account email address, and Customer may choose to terminate the Agreement by providing thirty days written notice and OpenAI will refund the prorated portion of paid fees. This termination right will not apply to updates made to features provided on a beta or evaluation basis.

3. Customer Obligations.

3.1. Customer Account. Customer must provide accurate and current Account information. Customer will not share Account access credentials or individual login credentials between multiple users. Customer may not resell or lease access to its Account or any End User Account. Customer will promptly notify OpenAI if it becomes aware of unauthorized access to the Account or the Services.

3.2. End Users. End User Accounts may only be provisioned to, registered for, and used by, a single End User. Customer is responsible for all activities that occur under its Account, including the activities of End Users with an End User Account or who access the Services through a Customer Application.

3.3. Restrictions. Customer will not, and will not permit End Users to: (a) use the Services or Customer Content in a way that violates applicable laws or OpenAI Policies; (b) use the Services or Customer Content in a way that violates third parties' rights; (c) allow non-enrolled minors to use OpenAI Services without consent from their parent or guardian; (d) Reverse Engineer any aspect of the Services or the systems used to provide the Services; (e) use Output to develop artificial intelligence models that compete with OpenAI's products and services; provided that Customer can use Output for a Permitted Use; (f) extract data from the Services other than as permitted through the Services; (g) buy, sell, or transfer API keys from, to, or with a third party; (h) interfere with or disrupt the Services, including circumvent any rate limits or restrictions or bypass any protective measures or safety mitigations for the Services; (i) violate or circumvent any Usage Limits or otherwise configure the Services to avoid Usage Limits.

3.4. Third-Party Services. Third-Party Services may be available through the Services, which Customer may elect to use in its sole discretion. By accessing a Third-Party Service, Customer agrees to the applicable Third-Party Service Terms. Customer's access or use of Third-Party Services are governed by this Agreement and the relevant Third-Party Service Terms.

4. Customer Content.

4.1. Generally. Customer and Customer's End Users may provide Input and receive Output. As between Customer and OpenAI, to the extent permitted by applicable law, Customer: (a) retains all ownership rights in Input; and (b) owns all Output. OpenAI hereby assigns to Customer all OpenAI's right, title, and interest, if any, in and to Output.

4.2. OpenAI Obligations. OpenAI will process and store Customer Content in accordance with the DPA. OpenAI will only use Customer Content as necessary to provide Customer with the Services, comply with applicable law, and enforce the OpenAI Policies. OpenAI will not use Customer Content to develop or improve the Services, unless Customer explicitly agrees to such use.

4.3. Customer Obligations. Customer is responsible for all Input and represents and warrants that it has all rights, licenses, and permissions required to provide Input to the Services. Customer is solely responsible for all use of the Outputs and for evaluating the accuracy and appropriateness of Output for Customer's use case.

4.4. Similarity of Output. Due to the nature of OpenAI's Services and artificial intelligence generally, Output may not be unique, and other users may receive similar content from OpenAI's services. Responses that are requested by and generated for other users are not considered Customer's Output.

5. Security.

5.1. Security Measures. OpenAI will comply with the Security Measures. OpenAI may periodically update the Security Measures. OpenAI will provide Customer with at least sixty days prior notice if OpenAI updates the Security Measures in a manner that materially diminishes the administrative, technical, or physical security features of the Services taken as a whole. Within five business days of receipt of this notice, Customer may elect to terminate the Agreement and associated Order Forms by providing written notice to OpenAI . OpenAI will refund the prorated portion of paid fees. Additional information regarding OpenAI's security practices for the Services is contained in the Security Resources.

5.2. Audit Reports. OpenAI has completed audits, conducted by an independent auditor, that evaluated the design and effectiveness of OpenAI security policies, procedures, and controls for the Services. Upon Customer's written request, but no more than once per year, OpenAI will provide Customer a copy of the most recent Audit Reports, which will be deemed OpenAI Confidential Information.

5.3 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; or
(b) uses illegal drugs.

5.3. 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.

5.4. Background Checks. Contractor shall maintain comprehensive hiring policies and procedures which include, among other things, a background check for criminal convictions 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).

5.5. 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 customer data, including University Data ("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.

5.6. Risk Assessments
   a. Self-Assessment. Contractor shall conduct risk assessments and/or audits of its use of customer data, including 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. To the extent required by applicable law, 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 by an independent third party, 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.

5.7. Data Encryption. Contractor warrants that all electronic data will be encrypted in transmission (including via web interface) and stored at no less than 128-bit level encryption. Contractor warrants that all University Data shall be securely destroyed, when destruction is requested by CSU.

5.8. 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).

5.9. 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.

5.10. 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.

5.11. 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 Agreement, including following termination of this Contract, subject to applicable law or regulation. 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.

5.12. CSU Data

(a) California Consumer Privacy Act (CCPA)
Contractor warrants that it complies with the CCPA and other California laws regarding data privacy. For purposes of this section only, "personal information" shall have the same meaning as that term is defined in the CCPA. If Contractor meets the definition of a "Business" under the CCPA, Contractor shall comply with the following obligations:

(b) Personal Information. Contractor will only collect, use, retain, or disclose personal information for the contracted business purposes.

(c) Use. Contractor will not collect, use, retain, disclose, sell, or otherwise make personal information available for Contractor's own commercial purposes or in a way that does not comply with the CCPA. If a law requires the Contractor to disclose personal information for a purpose unrelated to the contracted business purpose, the Contractor must first inform CSU of the legal requirement and give CSU an opportunity to object or challenge the requirement, unless the law prohibits such notice.

(d) Purpose. Contractor shall limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the contracted business purposes or another compatible operational purpose.

(e) Prompt Response. Contractor shall promptly comply with any request or instruction from a software user or from CSU requiring the Contractor to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing.

(f) Notice. If the contracted business purposes require the collection of personal information from individuals on CSU's behalf, Contractor will always provide a CCPA-compliant notice addressing use and collection methods.

(g) Statutory Compliance. Contractor shall comply with applicable state, Federal, and non-U.S. privacy laws, which may include but is not limited to the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)) ("GLBA"), the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) ("FERPA"), the IPA, the Health Insurance Portability and Accountability Act (110 Stat. 1936) ("HIPAA"), and the California Consumer Privacy Act (CA Civil Code 1798.100 *et seq.*). Contractor shall use best efforts, consistent with guidance from the Federal Trade Commission, the California Office of the Attorney General, the California Privacy Protection Agency, and other applicable guidance, to protect University Data from identity theft, fraud and unauthorized use. Contractor shall comply with all requirements governing redisclosure of education records, as that term is defined in FERPA.

(h) Permissible Use of Data

1. License to Use CSU Data. All rights, including all intellectual property rights, in and to University Data shall remain the exclusive property of CSU, and Contractor has a limited, nonexclusive license to use such data as provided in this Contract solely for the purpose of performing its obligations pursuant to the Contract, and only to the extent necessary to carry out its obligations to CSU under the terms of the Contract.
2. No Pecuniary Gain. Contractor shall not utilize any University Data for pecuniary gain not contemplated by this Contract, regardless of whether Contractor is or is not under contract at the time such gain is realized.
3. Disclosure of Data. Contractor may disclose University Data only to the extent necessary to carry out its obligations to CSU under the terms of the Contract, and shall not share such data with or disclose it to any third party without the prior written consent of CSU, except as required by law or permitted in this Contract. Contractor may only disclose University Data to affiliates or subcontractors for the purposes set forth in this Contract and only after the affiliates or subcontractors agree in writing to be bound by the same or equivalent restrictions, conditions, and requirements that apply to Contractor under this Contract.

(i) Confidentiality of Data

1. Duty of Confidentiality. Contractor shall maintain the confidentiality and privacy of Personal Information, Protected Data, and all other information designated "confidential" by CSU, to which Contractor has access, during the Term and after termination of the Contract. For purposes of this Contract, "Personal Information" shall have the same meaning as that term is defined in the Information Practices Act (California Civil Code, § 1798 *et seq.*) (the "IPA"), and "Protected Data" shall have the same meaning as defined in the CSU Information Security Policy and Standards, section VI (which, for clarification, includes both "Level 1 - Confidential" data and "Level 2 - Internal Use" data). Collectively, Personal Information, Protected Data, and all other information designated "confidential" by CSU, and to which Contractor has access, are collectively referred to in this Contract as "University Data". Contractor acknowledges the privacy rights of individuals to their personal information that are expressed in the IPA and in California Constitution Article 1, Section 1.

2. Notice of Subpoenas. Except as otherwise expressly prohibited by law, Contractor shall:
   A. immediately notify CSU in writing of any threatened or actual subpoenas, warrants, or other legal orders, demands or request received by Contractor seeking University Data, and
   B. Before making any disclosure of University Data, cooperate with CSU's requests in connection with efforts by CSU to intervene and quash or modify the legal order, demand, or request.

3. Return or Destruction of Data. Within thirty (30) days of termination or expiration of this Contract, or at any time upon the request of CSU, Contractor and its agents and subcontractors shall:
   A. provide CSU staff with the opportunity and ability to download /export University Data for records retention purposes;

B. destroy all University Data received from CSU and/or any retained by any of its affiliates, agents, representatives, or subcontractors, in any form, and delete from any computer system, retaining no copies of such information; and

C. Provide written certification to CSU that these actions have been completed.

Contractor agrees that all paper, film, or other hard copy media shall be shredded or destroyed such that it may not be reconstructed, and University Data shall be purged or destroyed in accordance with NIST Guidelines for media sanitization (https://csrc.nist.gov/). If Contractor determines that return or destruction of University Data is not feasible, Contractor shall extend the protections of this Addendum to such information, and shall limit further uses and disclosures to those purposes that make the return or destruction of the University Data infeasible; and Contractor's obligations under this Addendum shall survive the termination of the Contract.

4. Contractor's failure to comply with any provision of this section shall constitute a material breach of this contract.

5.13. Unauthorized Disclosure of Data

(a) Report to CSU. Contractor shall report, in writing, to csuciso@calstate.edu any use or disclosure of University Data not authorized by this Contract or in writing by CSU ("Security Incident"). This report shall:
   (1) be made without undue delay, but no later than seventy-two (72) hours from becoming aware of such unauthorized access.;
   (2) include details relating to any known or suspected security breach of Contractor's system or facilities which contain University Data, or any other breach of University Data relating to this Contract; and
   (3) identify:
      A. the nature of the unauthorized use or disclosure,
      B. the time and date of incident,
      C. a description of University Data used or disclosed,
      D. who made the unauthorized use or received the unauthorized disclosure,
      E. the actions Contractor has taken or will take to mitigate any potentially harmful effect of the unauthorized use or disclosure,
      F. the corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure, and
      G. such other information in the written report as reasonably requested by CSU.

(b) Cooperation. Contractor shall cooperate with CSU and its agents and provide reasonable information in its possession or in the possession of any of its affiliates and subcontractors to assist CSU in meeting its obligations to investigate and respond to the Security Incident, which may include allowing CSU staff to access log information and other pertinent information related to any investigation related to such breach or unauthorized use or disclosure. Contractor shall cooperate with any litigation or investigation proceedings concerning University Data loss or other breach of Contractor's obligations under this Contract.

(c) Notice to Affected Parties. Contractor shall fully cooperate with CSU with the preparation and transmittal of any notice, that CSU may deem appropriate or required by law, to be sent to affected parties regarding the known or suspected Security Incident. If directed by CSU, Contractor shall be administratively responsible for providing such notification in the most expedient time possible, consistent with the methods prescribed in California Civil Code §§ 1798.29 and 1798.82.

(d) Financial Responsibility. Contractor shall reimburse CSU in full for all costs incurred by CSU in investigation and remediation of a Security Incident, including but not limited to providing notification to individuals whose Personal Information was compromised, and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if University Data exposed during the breach could be used to commit identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the security breach. Contractor shall be financially responsible for any notice to affected parties resulting from Contractor's, its Representatives', its Affiliates', or its Subcontractors' acts or omissions with regard to the data security requirements of this Contract.

(e) Remedial Action. In the event of an unauthorized disclosure of data, Contractor shall take appropriate remedial action with respect to the integrity of its security systems and processes.

6. Payment.

6.1. Fees. Customer will pay OpenAI the applicable Fees in the currency and pursuant to the payment terms on the Order Form. Customer authorizes OpenAI to charge Customer for all applicable Fees using the payment method on the Account. Fees are non-refundable except as required by law or as otherwise specifically permitted in the Agreement. If Customer's Order Form includes a minimum commitment, the minimum commitment amount is non-cancellable except as required by law or as otherwise specifically permitted in the Agreement.

6.2. Payment. Customer will pay OpenAI invoices on the payment interval set forth in the Order Form. OpenAI may suspend or terminate the Services if Fees are past due. Customer will provide complete and accurate billing and contact information to OpenAI. OpenAI may reasonably change the date on which the charge is posted.

6.3. Taxes. Fees are exclusive of, and Customer is responsible for, all taxes. OpenAI will charge taxes when required to do so.

OpenAI will use Customer's "ship to" address in its Account as the place of supply for tax purposes.

6.4. Disputes. To dispute an invoice Customer must: (a) contact ar-enterprise@openai.com within thirty days of the date the disputed invoice was issued; and (b) pay all undisputed amounts. Overdue undisputed amounts may be subject to a finance charge of 1.5% of the unpaid balance per month.

7. Privacy. If Customer uses the Services to process "personal data" or "Personal Information" as defined under applicable data privacy and protection laws, Customer will: (a) provide legally adequate privacy notices and obtain necessary consents for the processing of personal data or Personal Information by the Services; (b) process personal data in accordance with applicable law; and (c) comply with the DPA.

8. HIPAA. If Customer uses the Services to create, receive, maintain, transmit, or otherwise process Protected Health Information, it will comply with the Healthcare Addendum. NOTWITHSTANDING THE FOREGOING, NOT ALL SERVICES OFFERED BY OPENAI ARE DESIGNED FOR PROCESSING PROTECTED HEALTH INFORMATION. IF CUSTOMER USES A SERVICE THAT IS NOT DESIGNED FOR PROCESSING PROTECTED HEALTH INFORMATION, CUSTOMER MAY NOT USE THE SERVICES TO STORE, TRANSMIT, OR PROCESS THIS INFORMATION.

9. Confidentiality.

9.1. Use and Nondisclosure. Recipient agrees it will: (a) only use Discloser's Confidential Information to exercise its rights and fulfill its obligations under this Agreement; (b) take reasonable measures to protect the Confidential Information; and (c) not disclose the Confidential Information to any third party except as expressly permitted in this Agreement. OpenAI acknowledges and agrees that this obligation extends to any "Protected Data" (as defined in Customer's policies here- https://calstate.policystat.com/policy/15698973/latest/) provided by Customer. OpenAI further agrees that its data security measures will be no less protective, with respect to Customer Confidential Information, than the level of protection OpenAI uses or would use in good faith to secure its own data of a similar type.

9.2. Exceptions. The obligations in Section 9.1 do not apply to information that: (a) is or becomes generally available to the public through no fault of Recipient nor by means of unauthorized access or disclosure of information; (b) was in Recipient's possession or known by it prior to receipt from Discloser; (c) was rightfully disclosed to Recipient without restriction by a third party; or (d) was independently developed without use of Discloser's Confidential Information.

9.3. Permitted Disclosure. Recipient may disclose Confidential Information only to its employees, contractors, and agents who have a need to know and who are bound by confidentiality obligations at least as restrictive as those in this Agreement. Recipient will be responsible for any breach of this Section 9 by its employees, contractors, and agents. Recipient may disclose Confidential Information to the extent required by law, if Recipient uses reasonable efforts to notify Discloser, to the extent permitted, prior to doing so. OpenAI acknowledges that this Agreement will be subject to examination and audit by: the CSU Office of the University Auditor, or its designated agent, and by the California State Auditor, or its designated agent, for a period of three (3) years after final payment under the Contract. Such examinations and audits shall be confined to those matters connected with the performance of the Contract, including, but not limited to, the costs of administering the Agreement.

9.4. The Comptroller General of the United States or designated federal authority for a period of up to five (5) years after final payment under the contract in the event the underlying contract is paid for in whole or in part by a federal contract or grant.

9.5. Remedies. The Receiving Party acknowledges that a disclosure of Confidential Information in violation of these terms would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore upon any such disclosure by the Receiving Party the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

10. Suspension.

10.1. Of End User Accounts. If an End User: (a) violates the Agreement; or (b) causes, or will cause, a Security Emergency, then OpenAI may request that Customer suspend or terminate the relevant End User account. If Customer fails to promptly suspend or terminate the End User account, then OpenAI may do so.

10.2. Of the Services. OpenAI may suspend Customer's access to the Services if: (a) it is required to do so by law; (b) Customer violates the Agreement or OpenAI Policies and does not cure such violation; or (c) doing so is necessary to prevent or terminate a Security Emergency. OpenAI will use reasonable efforts to narrowly tailor the suspension to prevent or terminate the Security Emergency. If possible, OpenAI will: (i) use reasonable efforts to notify Customer and provide an opportunity to resolve the issue prior to suspension; and (ii) cooperate with Customer to promptly restore access to the Services once it verifies Customer has resolved the condition requiring suspension.

11. IP Rights.

11.1. Reservation of Rights. Except as expressly set forth herein, the Agreement does not grant: (a) OpenAI any IP Rights in Customer Content; or (b) Customer any IP Rights in the Services. Customer obtains only a limited right to use the Services, and no ownership rights are transferred to Customer or its End Users under this Agreement.

11.2. Limited Permission. Customer grants OpenAI only the limited rights that are reasonably necessary for OpenAI to deliver the Services. This limited permission also extends to subcontractors or sub-processors.

11.3. Intentionally omitted.

12. Term and Termination.

12.1. Agreement Term. The Agreement will remain in effect for the Term.

12.2. Termination. Either Party may terminate this Agreement, including all Order Forms, upon written notice if the other party: (a) materially breaches this Agreement and fails to cure the breach within thirty days after receipt of written notice; or (b) ceases its business operations or becomes subject to insolvency proceedings.

12.3. Effects of Termination. If this Agreement terminates: (a) the rights granted by OpenAI to Customer will cease immediately; and (b) OpenAI will delete all Customer Content from its systems within thirty days, unless OpenAI is legally required to retain it, or if Customer has agreed otherwise in writing. Termination or expiration will not affect any rights or obligations, including the payment of amounts due, which have accrued under this Agreement up to the date of termination. In addition, except for a termination by Customer for cause, if this Agreement terminates any unpaid minimum commitment amounts set forth on the Order form will become immediately due.

12.4. Survival. The following provisions will survive termination or expiration of the Agreement: 6.2 (Payment), 11 (IP Rights), 12.3 (Effects of Termination), 12.4 (Survival), 13 (Warranties; Disclaimers), 14 (Indemnification), 15 (Limitation of Liability), 17 (Miscellaneous).

13. Warranties; Disclaimer.

13.1. Warranties. OpenAI warrants that, during the Term, when used in accordance with this Agreement, the Services will conform in all material respects with the Documentation and that OpenAI has or will procure all permits, licenses and authorizations necessary to properly perform its obligations under this Agreement. Additionally, OpenAI warrants that it has the right to enter into this Agreement and that the Services will be performed in a professional manner by competent personnel, in accordance with prevailing industry standards. All warranties included herein inure to Customer and Customer's successors, assigns, agencies and other governmental End Users of the Services.

13.2. Disclaimer. SUBJECT TO SECTION 13.1, THE SERVICES ARE PROVIDED "AS IS.". TO THE EXTENT PERMITTED BY LAW, EXCEPT AS EXPRESSLY STATED IN THE AGREEMENT, OPENAI AND ITS AFFILIATES AND LICENSORS MAKE NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE, OR NON-INFRINGEMENT. OPENAI MAKES NO REPRESENTATION, WARRANTY OR GUARANTEE THAT SERVICES WILL MEET CUSTOMER'S REQUIREMENTS OR EXPECTATIONS, THAT CUSTOMER CONTENT WILL BE ACCURATE, THAT DEFECTS WILL BE CORRECTED, OR REGARDING ANY THIRD-PARTY SERVICES. OPENAI WILL NOT BE RESPONSIBLE OR LIABLE FOR ANY CUSTOMER CONTENT, THIRD-PARTY SERVICES, THIRD-PARTY CONTENT, OR NON-OPENAI SERVICES (INCLUDING FOR ANY DELAYS, INTERRUPTIONS, TRANSMISSION ERRORS, SECURITY FAILURES, AND OTHER PROBLEMS CAUSED BY THESE ITEMS).

13.3. Beta Services. Despite anything to the contrary in the Agreement: (a) Customer may choose to use Beta Services in its sole discretion; (b) Beta Services may not be supported and may be changed at any time without notice; (c) Beta Services may not be as reliable or available as the Services; (d) Beta Services have not been subjected to the same Security Measures and auditing as the Services; and (e) OPENAI WILL HAVE NO LIABILITY ARISING OUT OF OR IN CONNECTION WITH BETA SERVICES – USE AT YOUR OWN RISK.

13.4. OpenAI warrants that no gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by OpenAI, or any agent or representative of OpenAI, to any officer or employee of Customer with a view toward securing the Agreement or securing favorable treatment with respect to any determinations concerning the performance of the Agreement. For breach or violation of this warranty, Customer shall have the right to terminate the Agreement, either in whole or in part, and any loss or damage sustained by Customer in procuring on the open market any items that OpenAI agreed to supply shall be borne and paid for solely by OpenAI. Customer's rights and remedies provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law, equity or under the Agreement.

14. Indemnification.

14.1. By OpenAI. OpenAI agrees to indemnify, defend, and hold Customer harmless against any liabilities, damages and costs (including reasonable attorneys' fees) payable to a third party arising out of a Claim alleging that the Services infringe any third-party IP Right. This excludes claims to the extent arising from: (a) combination of any Services with products, services, or software not provided by OpenAI or on OpenAI's behalf; (b) modification of any Services by any party other than OpenAI; (c) Customer Content; (d) Customer Applications (if any and the claim would not have arisen but for the Customer Application). In addition, the Service-Specific Terms Indemnity, as of the Effective Date, is included in this Agreement, is not subject to any liability cap, and OpenAI may not materially reduce Customer's protections under the Service-Specific Terms Indemnity without Customer's written agreement.

14.2. By Customer. Solely to the extent permitted by applicable law, Customer agrees to indemnify, defend, and hold OpenAI and its affiliates and licensors harmless against any liabilities, damages, and costs (including reasonable attorneys' fees) payable to a third party arising out of a Claim related to: (a) use of the Services in violation of this Agreement; (b) Customer Applications, if any; or (c) Input.

14.3. Mitigation. If OpenAI reasonably believes that all or any portion of the Services is likely to become the subject of an infringement Claim, OpenAI will: (a) obtain, at OpenAI's expense, the right for Customer to continue using the Services in accordance with this Agreement; (b) replace or modify the allegedly infringing Service; or (c) if (a) and (b) are not commercially practicable, OpenAI may, in its sole discretion, terminate this Agreement upon written notice to Customer and refund any prepaid amounts for unused Services. Customer will promptly comply with all reasonable instructions provided by OpenAI with respect to the above, including any instruction to replace, modify, or cease use of the Service.

14.4. Procedure. A party seeking indemnity will provide the indemnifying party with prompt written notice upon becoming aware of any claim, reasonable cooperation in the defense of or investigation of the claim and allow the indemnifying party sole control of defense and settlement of the claim including selection of counsel, provided that the party seeking indemnity is entitled to participate in its own defense at its sole expense. The indemnifying party cannot enter any settlement or compromise of any claim without prior written consent of the other party, which will not be unreasonably withheld, except that the indemnifying party may without consent enter any settlement of a claim that resolves the claim without liability to the other party, impairment to any of the other party's rights, or requiring the other party to make any admission of liability. THE INDEMNITIES ARE A PARTY'S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY THE OTHER PARTY OF A THIRD PARTY'S IP RIGHTS.

15. Limitation of Liability.

15.1. Limitation on Indirect Liability. TO THE FULLEST EXTENT PERMITTED BY LAW, EXCEPT FOR: (A) A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; (B) CUSTOMER'S BREACH OF SECTION 3.3 (RESTRICTIONS); (C) OPENAI'S BREACH OF SECTION 5 (SECURITY), OR (D) EITHER PARTY'S BREACH OF SECTION 9 (CONFIDENTIALITY), NEITHER CUSTOMER NOR OPENAI OR EITHER PARTY'S AFFILIATES OR LICENSORS WILL BE LIABLE UNDER THIS AGREEMENT FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING LOST PROFITS, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

15.2. Limitation on Amount of Liability. TO THE FULLEST EXTENT PERMITTED BY LAW, EXCEPT FOR: (A) A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, (B) EITHER PARTY'S BREACH OF CONFIDENTIALITY (SECTION 9) OR (C) A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT, EACH PARTY'S TOTAL LIABILITY UNDER THE AGREEMENT WILL NOT EXCEED THE TOTAL AMOUNT CUSTOMER PAID TO OPENAI DURING THE TWELVE MONTHS IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO LIABILITY. THE FOREGOING LIMITATIONS APPLY DESPITE ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

16. Intentionally Omitted

17. CSU Insurance Requirements

Contractor shall not commence the Contracted Work until it has obtained all the insurance required by this Contract, and such insurance has been approved by CSU.

Policies and Coverage

(a) Required. Contractor shall obtain and maintain the following policies and coverage:
   (1) Comprehensive or Commercial General Liability Insurance, on an occurrence basis, covering Contracted Work done or to be done by or on behalf of the Contractor and providing insurance for bodily injury, personal injury, property damage, and contractual liability. CSU may require the aggregate limit to apply specifically to the Contracted Work in certain circumstances, and will notify Contractor of this requirement.
   (2) Business Automobile Liability Insurance on an occurrence basis, covering owned, hired, and non-owned automobiles used by or on behalf of Contractor and providing insurance for bodily injury, property damage, and contractual liability. Such insurance shall include coverage for uninsured and underinsured motorists.
   (3) Worker's Compensation, including Employers Liability Insurance as required by law.

(b) Additional. Contractor shall also be required to obtain and maintain the following policies and coverage to the extent indicated below:
   (1) Environmental Impairment Liability or Pollution Liability Insurance in the event that the Contracted Work involves hazardous materials which could result in any loss, cost or expense arising out of any requirement to clean up, remove, contain, treat, detoxify or in any way respond to pollutants or injury or damage resulting therefrom. This includes, but is not limited to, Contracted Work involving asbestos, lead, fuel storage or pipes, sewage, industrial waste, and hazardous chemicals (such as pesticides, carcinogens, trichloroethylene (TCE), or polychlorinated biphenyls (PCBs).

(2) Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability Insurance in the event that the Contracted Work involves access to or storage of Protected Data. For purposes of this Contract, "Protected Data" has the same meaning as defined in the CSU Information Security Policy and Standards, section VI (which, for clarification, includes both "Level 1 - Confidential" data and "Level 2 - Internal Use" data). Such insurance shall cover liabilities for financial loss, damages, and/or costs incurred as a result of any confirmed or suspected data security breach or loss of Protected Data (including personally identifiable information) due to the acts, omissions, and/or intentional misconduct of Contractor, its officers, employees, agents, sub-contractors, or anyone acting on behalf of Contractor in connection with the performance of this Contract. Such coverage shall include without limitation, all of the following:

A. Costs to notify persons whose data were lost or compromised
B. Costs to provide credit monitoring and credit restoration services to persons whose data were lost or compromised
C. Costs associated with third party claims arising from a confirmed or suspected data security breach or loss of CSU confidential data, including litigation costs and settlement costs
D. Any investigation, enforcement, fines and penalties, or similar miscellaneous costs arising from a confirmed or suspected data security breach or loss of CSU confidential data
E. Any payment made to a third party as a result of extortion related to a confirmed or suspected data security breach or loss of CSU confidential data

(3) Professional Liability Insurance if the Contracted Work involves professional services involving specialized skill or training, including but not limited to:

A. preparation of any map, shop drawing, opinion, report, survey, field order, change order, design, drawing, specification, recommendation, warning, permit application, payment request, manual or inspection;
B. supervision, inspection, quality control, architectural, engineering or surveying activity or service;
C. job site safety;
D. construction contracting, construction administration, or construction management;
E. computer consulting or design, software development or programming service;
F. selection of a contractor or subcontractor;
G. real estate, legal, medical, employment, investment, or management services;
H. monitoring, testing, or sampling services; or
I. if otherwise directed by CSU in writing.

(4) Other insurance as agreed upon by CSU and Contractor.

(c) Verification of Coverage. Contractor shall submit original certificates of insurance and endorsements to the policies of insurance required by the Contract to CSU as evidence of the insurance coverage. Renewal certifications and endorsements shall be timely filed by Contractor for all coverage until the Contracted Work is accepted as complete. CSU reserves the right to require Contractor to furnish CSU complete, certified copies of all required insurance policies.

(d) Required Provisions. Nothing in these insurance provisions shall be deemed to alter the indemnification provisions in this Contract. The insurance policies shall contain, or be endorsed to contain, the following provisions.

1. The general and automobile liability policies shall name the State of California, CSU, the Trustees of the California State University, and their officers, employees, representatives, volunteers, and agents as additional insureds. Such endorsement shall be on an ACORD certificate or similar form for this purpose; a statement on the certificate itself does not satisfy this requirement.
2. For any claims related to the Contracted Work, Contractor's insurance coverage shall be primary insurance as respects the State of California, CSU the Trustees of the California State University, and their officers, employees, representatives, volunteers, and agents. Any insurance or self-insurance maintained by the State of California, CSU, the Trustees of the California State University, and their officers, employees, representatives, volunteers, and agents shall be in excess of Contractor's insurance and shall not contribute with it.
3. Each insurance policy required by this section shall state that coverage shall not be canceled by either Contractor or the insurance carrier, except after thirty (30) days prior written notice by certified mail, return receipt requested (or other written notice with proof of receipt), has been given to CSU.
4. The State of California, CSU, the Trustees of the California State University, and their officers, employees, representatives, volunteers, and agents shall not by reason of their inclusion as additional insureds incur liability to the insurance carriers for payment of premiums for such insurance.
5. Each insurance policy required by this section shall contain an endorsement providing a waiver of transfer of rights of recovery against others (waiver of subrogation) as to the State of California, CSU, the Trustees of the California State University, and their officers, employees, representatives, volunteers, and agents.

Amount of Insurance

(e) Minimum Coverage. The limits stated below are minimum required amounts of insurance coverage but do not serve to limit amounts recoverable by CSU. CSU is entitled to any valid and collectible insurance and any other sources of recovery. The insurance furnished by Contractor under this Contract shall provide coverage in amounts not less than the following:

1. Comprehensive or Commercial General Liability Insurance—Limits of Liability
    A. $4,000,000 General Aggregate
    B. $2,000,000 Each Occurrence—combined single limit for bodily injury and property damage.
    C. $2,000,000 Each Person/Entity for personal liability
    D. $2,000,000 for contractual liability
2. Business Automobile Liability Insurance—Limits of Liability
    A. $1,000,000 Each Accident—combined single limit for bodily injury and property damage to include uninsured and underinsured motorist coverage.
3. Workers' Compensation—limits as required by law with Employers Liability limits of $1,000,000.

(f) Cyber. For Contracts involving Contractor access to or storage of Protected Data, Contractor shall obtain the additional coverage in amounts not less than the following, unless a different amount is agreed upon in writing signed by Contractor and CSU:

1. Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability Insurance – Limits of Liability

    A. $10,000,000 General Aggregate
    B. $10,000,000 Each Occurrence

(g) Professional Services. For Contracts involving professional services, Contractor shall obtain the additional coverage in amounts not less than the following, unless a different amount is agreed upon in writing signed by Contractor and CSU:

1. Professional Liability Insurance – Limits of Liability
    A. $5,000,000 General Aggregate
    B. $5,000,000 Each Claim

Acceptability of Insurers

Insurers shall be licensed by the State of California to transact insurance and shall hold a current A.M. Best's rating of A:VII, or shall be a carrier otherwise acceptable to CSU.

Subcontractor's Insurance

Contractor shall ensure that its subcontractors are covered by insurance of the types required by this Contract, and that the amount of insurance for each subcontractor is appropriate for that subcontractor's work as relates to this Contract. Contractor shall not allow any subcontractor to commence work on its subcontract until the insurance has been obtained and approved by CSU. Only the Contractor and its hazardous materials subcontractor(s) are required to have the coverage for projects involving hazardous materials.

Miscellaneous

(a) Any deductible under any policy of insurance required in this Contract shall be Contractor's liability.
(b) Acceptance of certificates of insurance by CSU shall not limit Contractor's liability under the Contract.
(c) In the event Contractor does not comply with these insurance requirements, CSU may, at its option, provide insurance coverage to protect CSU. The cost of the insurance shall be paid by Contractor and, if prompt payment is not received, may be deducted from Contract sums otherwise due the Contractor.
(d) If CSU is damaged by Contractor's failure to provide or maintain the required insurance, Contractor shall pay CSU for all such damages.
(e) Except as specifically provided for in contracts involving hazardous materials, Contractor's obligations to obtain and maintain all required insurance are non-delegable duties under this Contract.

18. Miscellaneous.

18.1. Entire Agreement. This Agreement is the entire agreement between Customer and OpenAI with respect to its subject matter and supersedes all prior or contemporaneous agreements, communications and understandings, whether written or oral. This Agreement hereby incorporates by this reference the OpenAI Policies and relevant Order Forms. Customer agrees that any terms and conditions contained in any purchase order Customer sends to OpenAI will not apply to this Agreement and are null and void.

18.2. Conflicting Terms. If there is a conflict between the documents that make up the Agreement, the documents will control in the following order, the: (a) Service-Specific Terms; (b) Agreement; (c) OpenAI Policies and (d) the applicable Order Form.

18.3. Governing Law. This Agreement will be governed by the laws of the State of California, excluding California's conflicts of

law rules or principles. All claims arising out of or relating to this Agreement will be brought exclusively in the federal or state courts of San Francisco County, California, USA.

18.4. Severability. Unenforceable provisions will be modified to reflect the parties' intention and only to the extent necessary to make them enforceable, and the remaining provisions of the Agreement will remain in full effect.

18.5. Notices. Notices must be sent via email, first class, airmail, or overnight courier and are deemed given when received. Notices to Customer may also be sent to the following: (Name: Michael Trullinger, Email: mtrullinger@calstate.edu Contract Services and Procurement; as well as the applicable Account email address and are deemed given when sent. Notices to OpenAI must be sent to OpenAI Legal at contract-notices@openai.com, with a copy to: (a) if OpenAI, L.L.C., 1455 3rd Street, San Francisco, California 94158; or (b) if OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland.

18.6. Waiver. A waiver of any default is not a waiver of any subsequent default.

18.7. Assignment. This Agreement cannot be assigned other than as permitted under this Section 17.7 (Assignment). OpenAI may assign this Agreement to an Affiliate without notice or Customer consent. Either Party may assign this Agreement to a successor to substantially all the respective party's assets or business, provided the assigning party provides at least thirty days prior written notice of the assignment. This Agreement will be binding upon the parties and their respective successors and permitted assigns.

18.8. No Agency. OpenAI and Customer are not legal partners or agents but are independent contractors.

18.9. Force Majeure. Except for payment obligations, neither Customer nor OpenAI will have any liability for failures or delays resulting from conditions beyond Customer's or OpenAI's reasonable control, including but not limited to governmental action or acts of terrorism, earthquake or other acts of God, labor conditions, or power failures.

18.10. No Third-Party Beneficiaries. There are no intended third-party beneficiaries to this Agreement, and it is Customer and OpenAI's specific intent that nothing contained in this Agreement will give rise to any right or cause of action, contractual or otherwise, in or on behalf of any third party.

18.11. U.S. Federal Agency Entities. The Services were developed solely at private expense and are commercial computer software and related documentation within the meaning of the applicable U.S. Federal Acquisition Regulation and agency supplements thereto.

18.12. Trade Controls. Customer is solely responsible for ensuring that its use of the Services complies with applicable trade laws, including sanctions and export control laws. Customer's Input may not include material or information that requires a government license for release or export. Customer may not use the Services in or for the benefit of, or export or re-export the Services to, any U.S. embargoed countries or to anyone on a Restricted Party List. Customer represents and warrants that Customer and End Users are not located in any U.S. embargoed countries, are not identified on any Restricted Party List, and that Customer will comply with applicable export control laws, including any "know your customer" requirements or obligations applicable to Customer's End Users.

18.13. Geographical Limitations on Use. Customer and End Users may not access or offer access to the Services outside of the Supported Countries and Territories. A violation of this Section 17.13 may result in Services suspension under Section 10.

18.14. Sovereign immunity. Nothing in this contract is intended by the CSU to waive sovereign immunity or any other defenses or immunities afforded by any or all U.S. federal law, California state law, and other applicable law. Notwithstanding any provision to the contrary in the DPA, this provision takes precedence over all other provisions in the contract and the DPA. To the extent that Customer reasonably believes and can credibly substantiate that OpenAI's processing creates sovereign immunity risk, Customer may provide OpenAI with written notice to that effect (a "Substantiated Sovereign Immunity Concern"). Upon receipt of a Substantiated Sovereign Immunity Concern, OpenAI will have sixty (60) days to cure such concern; if OpenAI cannot cure Customer's concern (as determined by Customer, in its reasonable discretion), then Customer may terminate this Agreement for convenience and OpenAI will refund the prorated portion of paid fees.

18.15. Processing location. To the extent possible, OpenAI agrees to permanently store Customer Content at rest within the United States.

18.16. Additional OpenAI Obligations.

A. OpenAI certifies and declares it is not engaged in business within this State of California to sell or use any article or product as a "loss leader" as defined in Section 17030 of the Business and Professions Code section 17030.

B. OpenAI declares and certifies that it is not an expatriate corporation and is not precluded from contracting with CSU by The California Taxpayer and Shareholder Protection Act of 2003, Public Contract Code Section 10286, et seq.

C. By accepting a contract with Customer, OpenAI certifies neither it nor its principals or its subcontractors are presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participating in this

transaction by any federal department or agency, in accordance with the Office of Management and Budget guidelines at 2 C.F.R. Part 180 that implement Executive Orders 12549 (3 C.F.R. Part 1986 Comp., p. 189) and 12689 (3 C.F.R. Part 1989 Comp., p. 235). OpenAI shall provide immediate written notice to Customer if, at any time, OpenAI learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

D. Conflict of Interest

CSU requires a Statement of Economic Interests (California Form 700) to be filed by any Contractor who is involved in the making or participates in the making of decisions which may foreseeably have a material effect on any financial interest of CSU. The parties acknowledge and agree that, as of the Effective Date, Contractor will not participate in any such decision.

E. Appropriation of Funds

If the term of this Contract continues into fiscal years subsequent to the fiscal year in which it is approved, such continuation is subject to the appropriation of funds for such purpose by the state legislature. If funds to continue payment are not appropriated, Contractor agrees to take back any commodities furnished under the Contract and not yet paid for by CSU, terminate any future services and/or commodities to be supplied to CSU under the Contract, and to relieve CSU of any further obligation.

F. Follow-On Contracts

No person, firm, or subsidiary thereof who has been awarded a contract for Consulting and Direction (as defined in this section) shall be awarded a contract for the provision of services, or any other related action that is required, suggested, or otherwise deemed appropriate in the end product of the consulting services contract.

(a) If Contractor or its affiliates provides Consulting and Direction, Contractor, and its affiliates:
   (1) shall not be awarded a subsequent Contract to supply the service or system, or any significant component thereof, that is used for, or in connection with, any subject of such Consulting and Direction; and
   (2) shall not act as consultant to any person or entity that does receive a Contract described in sub-section (i). This prohibition will continue for one (1) year after termination of this Contract or completion of the Consulting and Direction, whichever is later.

(b) "Consulting and Direction" means services for which Contractor received compensation from CSU includes:
   (1) development of, or assistance in the development, of work statements, specifications, solicitations, or feasibility studies;
   (2) development or design of test requirements;
   (3) evaluation of test data;
   (4) direction of or evaluation of another contractor;
   (5) provision of formal recommendations regarding the acquisition of products or services; or
   (6) provisions of formal recommendations regarding any of the above.

(c) For purposes of this Section, "affiliates" means employees, directors, partners, joint venture participants, parent corporations, subsidiaries, or any other entity controlled by, controlling, or under common control with Contractor; control exists when an entity owns or directs more than fifty percent (50%) of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority.

(a) Except as prohibited by law, the restrictions of this Section will not apply:
   (1) to follow-on advice given by vendors of commercial off-the-shelf products, including software and hardware, on the operation, integration, repair, or maintenance of such products after sale; or
   (2) where CSU has entered into a Contract for software or services and the scope of work at the time of Contract execution expressly calls for future recommendations among the Contractor's own products.

(b) The restrictions set forth in this Section are in addition to conflict of interest restrictions imposed on public Contractors by California law ("Conflict Laws"). In the event of any inconsistency, such Conflict Laws override the provisions of this Section, even if enacted after execution of this Contract.

G. Nondiscrimination

(a) Nondiscrimination. During the performance of this Contract, Contractor and its subcontractors shall not deny the Contract's benefits to any person on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status, nor shall they discriminate unlawfully against any employee or applicant for employment because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, reproductive health decision making, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status. Contractor shall ensure that the evaluation and treatment of employees and applicants for employment are free of such discrimination.

(b) Compliance. To the extent applicable, Contractor shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code, § 12900 et seq.), the regulations promulgated thereunder (Cal. Code Regs., tit. 2, § 11000 et seq.), the provisions of Article 9.5, Chapter 1, Part 1, Division 3, Title 2 of the Government Code (Gov. Code, §§ 11135- 11139.8), and the regulations or standards adopted by CSU to implement such article.

(c) Access. Contractor shall permit access by representatives of the Civil Rights Department and CSU upon reasonable notice at any time during the normal business hours, but in no case less than 24 hours' notice, to such of its books, records, accounts, and all other sources of information and its facilities as said Department or CSU shall require to ascertain compliance with this clause.

(d) Notice to labor organizations. Intentionally Omitted.

(e) Subcontracts. Intentionally Omitted.

H. Compliance with NLRB Orders

Contractor declares under penalty of perjury under the laws of the State of California that no more than one final, unappealable finding of contempt of court by a federal court has been issued against Contractor within the immediately preceding two-year period because of Contractor's failure to comply with an order of a federal court to comply with an order of the National Labor Relations Board.

I. Drug-Free Workplace Certification

Except in the case of credit card purchase of goods of $2,500 or less, Contractor certifies that Contractor shall comply with the requirements of the Drug-Free Workplace Act of 1990

J. Forced, Convict, Indentured and Child Labor

By accepting a contract with CSU, Contractor:

(a) certifies that no equipment, materials, or supplies furnished to CSU pursuant to this Contract have been produced in whole or in part by sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor, or with the benefit of sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor. Contractor further certifies it will adhere to the Sweat-free Code of Conduct as set forth on the California Department of Industrial Relations website located at https://www.dir.ca.gov/sweatfreecode.htm, and Public Contract Code section 6108.

(b) agrees to cooperate fully in providing reasonable access to its records, documents, agents or employees, or premises if reasonably required by authorized officials of the State, the Department of Industrial Relations, or the Department of Justice to determine Contractor's compliance with the requirements under paragraph (A).

K. Recycled Content Certification. – Intentionally Omitted

L. Entertainment Event Certification. – Intentionally Omitted

M. Child Support Compliance Act

For any contract in excess of $100,000, Contractor acknowledges in accordance with Public Contract Code section 7110, that:

(a) Contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable state and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with Section 5200) of Part 5 of Division 9 of the Family Code; and

(b) Contractor, to the best of its knowledge, is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.

N. Americans With Disabilities Act (ADA)

Contractor warrants that it complies with California and federal disabilities laws and regulations (including but not limited to the Americans with Disabilities Act of 1990, 42 U.S.C. 12101 et seq). Contractor hereby warrants the products or services it will provide under this Contract undergo third-party auditing with respect to the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194. Contractor agrees to share the results of such audits with Customer; in the event that such audit results demonstrate that the Services hereunder will directly prohibit Customer from its own legal accessibility requirements (a “Material Accessibility Deficiency”), Customer may provide written notice to OpenAI of such Material Accessibility Deficiency, upon receipt of which OpenAI will have ninety (90) days to cure such Material Accessibility

Deficiency. If OpenAI cannot cure in that period, as determined by Customer in its reasonable discretion, then Customer may terminate this Agreement for convenience. Customer will have the right to request, and OpenAI will provide, additional documentation, reviews, and accessibility demonstrations throughout the contract term and upon renewal.

O. Citizenship and Public Benefits
If Contractor is a natural person, Contractor certifies he or she is a citizen or national of the United States or otherwise qualified to receive public benefits under the federal Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (P.L. 104-193; 110 STAT. 2105, 2268-69).

P. DVBE and Small Business Participation. - Intentionally Omitted.

19. Definitions.

"Account" means an administrative account provided to Customer by OpenAI for the purpose of administering the Services.

"Administrator" means a Customer designated End User with administrative privileges.

"Account Console" means the online tool provided by OpenAI to Customer for use in administering the Services.

"Affiliate" means with respect to either Party, any other person or entity that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with, such specified person or entity.

"API" means OpenAI's application programming interface.

"Audit Reports" means the third-party audit reports for the Services.

"Authorized Purchaser" means a Customer employee designated by Customer to act as an authorized purchaser of the Services. Customer can designate Authorized Purchasers in an offline Order Form or in the Admin Console. Administrators are Authorized Purchasers. Authorized Purchasers may be periodically updated by Customer in the Account Console.

"Beta Services" means services or features identified as alpha, beta, preview, early access, or evaluation, or words or phrases with similar meanings.

"Confidential Information" means any business, technical or financial information, materials, or other subject matter disclosed by Discloser to Recipient that is: (a) identified as confidential at the time of disclosure; or (b) should be reasonably understood by Recipient to be confidential under the circumstances. Confidential Information includes Customer Content.

"Claim" means legal proceedings filed by a third party.

"Customer Application" means Customer's applications, products, or services.

"Customer Content" means the Input and the Output.

"Discloser" means the Party that discloses Confidential Information to the other under this Agreement.

"Dispute" means a claim by a Party arising out of or relating to this Agreement or the Services.

"Documentation" means the documentation OpenAI provides to Customer or otherwise makes publicly available.

"DPA" means the OpenAI data processing addendum attached as Exhibit A

"End User" means any party: (a) who accesses the Services under Customer's Account; or (b) who uses Customer Applications. End Users may include Customer's and its Affiliate's employees, consultants, customers, agents, representatives, students or any other person authorized by Customer to use the Services through Customer's Account.

"End User Account" means an account for an End User under Customer's Account.

"Feedback" means any feedback provided by Customer to OpenAI regarding the Services.

"Fees" means all fees charged to Customer's Account in accordance with an Order Form, or if an Order Form does not exist, then according to the Pricing Page.

"Healthcare Addendum" means the OpenAI Healthcare Addendum and Business Associate Agreement available at: cdn.openai.com/osa/healthcare-addendum.pdf.

"Initial Term" means the initial term for the Services beginning on the Start Date and continuing for the duration set forth on the Order Form.

"Input" means Customer and Customer's End Users input to the Services.

"IP Rights" means all registered or unregistered intellectual property rights throughout the world, including rights in patents, copyrights, trademarks, trade secrets, designs, databases, domain names, and moral rights.

"Marks" means the name, logo, or marks of a Party.

"NAM" means National Arbitration and Mediation.

"OpenAI Brand Guidelines" means the OpenAI guidelines available at: https://openai.com/brand.

"OpenAI Policies" means the Service-Specific Terms, Sharing and Publication Policy, and Usage Policies. The version of OpenAI Policies applicable to Customer will be those in effect on the most recent effective date between either the Agreement, Customer's most recent Order Form, or Services renewal. If Customer elects to use new Services added to the Service-Specific Terms after the most recent effective date in the preceding sentence, then the OpenAI Policies in effect as of that Customer use will apply.

"Order Form" means the ordering document signed by Customer and OpenAI or OpenAI webpage that Customer uses to purchase the Services.

"Output" means output from the Services based on the Input.

"Permitted Use" means Customer using Output to: (i) develop artificial intelligence models primarily intended to categorize, classify, or organize data (e.g., embeddings or classifiers), if these models are not distributed or made commercially available to third parties; and (ii) fine tune or customize models provided as part of OpenAI's fine-tuning or other Services set forth on the Pricing Page.

"Pricing Page" means the pages available at https://openai.com/api/pricing/ or https://openai.com/chatgpt/pricing/.

"Protected Health Information" is as defined under the HIPAA Privacy Rule (45 C.F.R. Section 160.103).

"Recipient" means the Party receiving Confidential Information from the Discloser.

"Renewal Term" means a renewal term for the Services following either the Initial Term, or a previous Renewal Term. Note that if Customer renews without a new Order Form, the duration of that Renewal Term will be the same duration of the immediately preceding Initial Term or Renewal Term.

"Restricted Party List" means the U.S. Office of Foreign Assets Control's ("OFAC") list of Specially Designated Nationals (aka the "SDN List"), the U.S. Bureau of Industry and Security's ("BIS") Denied Persons List and Entity List, and any other applicable restricted party lists promulgated by OFAC, BIS, or other agencies of comparable jurisdiction, inside or outside the U.S., now or in the future.

"Reverse Engineer" means reverse assemble, reverse compile, decompile, translate, engage in model extraction or stealing attacks, or otherwise attempt to discover the source code or underlying components of the Services, algorithms, and systems of the Services (except to the extent these restrictions are contrary to applicable law).

"Security Emergency" means use of the Services by Customer or a Customer End User that could reasonably result in a security risk, credible risk of harm, infringement of third-party rights, or liability to OpenAI, the Services, or a third party.

"Security Measures" means the security measures available at: cdn.openai.com/osa/security-measures.pdf

"Security Resources" means the content available at: https://trust.openai.com/.

"Services" means OpenAI's services for businesses, enterprises, or developers made available for purchase or use in Customer's Account, along with any of OpenAI's associated software, tools, developer services, documentation, and websites, but excluding any Third-Party Service.

"Services Term" means the Initial Term and all Renewal Terms.

"Service-Specific Terms" means the terms specific to certain services at: https://openai.com/policies/service-terms.

"Service-Specific Terms Indemnity" means OpenAI's indemnities included in the Service-Specific Terms.

"Sharing and Publication Policy" means the terms at: https://openai.com/policies/sharing-publication-policy.

"Start Date" means the date an Initial Term, or Renewal Term, begins. Start Dates are listed on the Order Form. Note that if Customer renews without a new Order Form, the Start Date for that Renewal Term will be calculated based on the original Start Date.

"Supported Countries and Territories" means the countries and territories for which OpenAI supports access to API Services and our ChatGPT services. These countries and territories are available at: https://help.openai.com/en/articles/5347006-openai-api-supported-countries-and-territories (for API) or https://help.openai.com/en/articles/7947663-chatgpt-supported-countries (for ChatGPT), and may be updated from time to time.

"Term" means the term of the Agreement, which will begin on the Effective Date and continue until the earlier of: (i) the end of the Services Term; or (ii) termination of the Agreement as set forth herein.

"Third-Party Services" means third party products, services, or content offered by third parties through the Services.

"Third-Party Service Terms" means any additional terms applicable to the Third-Party Service.

"Usage Limits" means End User, messaging, token, throughput rate, or other limits on Customer's use of the Services as described in the applicable Order Form or Documentation.

"Usage Policies" means the usage policies at: https://openai.com/policies/usage-policies.

This Data Processing Addendum ("DPA") governs OpenAI's processing of Customer Data (i) provided by Customer to OpenAI through OpenAI's API or any OpenAI services for businesses ("API Services") or (ii) pursuant to OpenAI's provision of the ChatGTPT Enterprise service for businesses (the "ChatGPT Enterprise Services") (for purposes of this DPA, the API Services and ChatGPT Enterprise Services are together the "Services") under the terms of the OpenAI Business Terms (located at openai.com/policies/business-terms), Enterprise Agreement, or other agreement between Customer and OpenAI governing Customer's use of the Services (the "Agreement") and is hereby incorporated into the Agreement. If and to the extent language in this DPA conflicts with the Agreement, the conflicting terms in this DPA shall control. Capitalized terms not defined in this DPA have the meaning set forth in the Agreement. For the purposes of this DPA only, "Customer" includes any affiliate entity of Customer's that (a) has entered into an Order Form with OpenAI and that (b) directly or indirectly, through one or more intermediaries controls, is controlled by, or is under common control with Customer. Notwithstanding anything herein to the contrary, nothing in this DPA shall be deemed a waiver of sovereign immunity of the State of California or the Customer.
If Customer is located in the EEA or Switzerland, OpenAI Ireland Ltd will provide the Services and contract with Customer. If Customer is located in the UK or anywhere else other than the EEA or Switzerland, OpenAI, LLC will provide the Services and contract with Customer. For the purposes of this DPA, "OpenAI" refers to the OpenAI entity contracting with Customer.

OpenAI and Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws (collectively, "Data Protection Laws") in connection with the Services. Data Protection Laws may include, depending on the circumstances, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("CCPA"), Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("CPA"), Connecticut's Data Privacy Act ("CTDPA"), Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("UCPA"), VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("VCDPA") (collectively "U.S. Privacy Laws"), and the United Kingdom and/or European Union General Data Protection Regulation (Regulation (EU) 2016/679) (collectively the "GDPR"), and applicable subordinate legislation and regulations implementing those laws.

In connection with the Agreement, Customer is the person that determines the purposes and means for which Customer Data (as defined below) is processed (a "Data Controller"), whereas OpenAI processes Customer Data in accordance with the Data Controller's instructions and on behalf of the Data Controller (as a "Data Processor"). "Data Controller" and "Data Processor" also mean the equivalent concepts under Data Protection Laws. For the purposes of the Agreement and this DPA, (i) "Personal Data" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws; and (ii) "Customer Data" means Personal Data that Customer provides to OpenAI that OpenAI processes on behalf of Customer to provide the Services. OpenAI will process Customer Data as Customer's Data Processor to provide or maintain the Services and for the purposes set forth in this DPA, the Agreement and/or in any other applicable agreements between Customer and OpenAI.

1. Processing Requirements

As a Data Processor, OpenAI agrees to:

a. process Customer Data only (i) on Customer's behalf for the purpose of providing and supporting OpenAI's Services (including to provide insights, reporting, analytics, and platform abuse, trust and safety monitoring); (ii) in compliance with the written instructions received from Customer; and (iii) in a manner that provides no less than the level of privacy protection required of it by Data Protection Laws;

b. promptly inform Customer in writing if OpenAI cannot comply with the requirements of this DPA;

c. not provide Customer with remuneration in exchange for Customer Data from Customer. The parties acknowledge and agree that Customer has not "sold" (as such term is defined by the CCPA) Customer Data to OpenAI;

d. not "sell" (as such term is defined by U.S. Privacy Laws) or "share" (as such term is defined by the CCPA) Personal Data;

e. inform Customer promptly if, in OpenAI's opinion, an instruction from Customer violates applicable Data Protection Laws;

f. require (i) persons employed by it and (ii) other persons engaged to perform on OpenAI's behalf to be subject to a duty of confidentiality with respect to the Customer Data and to comply with the data protection obligations applicable to OpenAI under the Agreement and this DPA;

g. engage the organizations or persons listed at https://platform.openai.com/subprocessors to process Customer Data (each "Subprocessor," and the list at the foregoing URL, the "Subprocessor List") to help OpenAI satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors. Customer hereby consents to the use of such Subprocessors. If Customer subscribes to email notifications as provided on the Subprocessor List website, then OpenAI will notify Customer of any changes OpenAI intends to make to the Subprocessor List at least 15 days before the changes take effect (which may be via email, a posting, or notification on an online portal for our services or other reasonable means). In the event that Customer does not wish to consent to the use of such additional Subprocessor, Customer may notify OpenAI that Customer does not consent within fifteen (15) days on reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Subprocessor List or by contacting privacy@openai.com. In such case, OpenAI shall have the right to cure the objection through one of the following options: (i) OpenAI will cancel its plans to use the Subprocessor with regards to processing Customer Data or will offer an alternative to provide its Services or services without such Subprocessor; (ii) OpenAI will take the corrective steps requested by Customer in Customer objection notice and proceed to use the Subprocessor; (iii) OpenAI may cease to provide, or Customer may agree not to use whether temporarily or permanently, the particular aspect or feature of the OpenAI Services or services that would involve the use of such Subprocessor; or (iv) Customer may cease providing Customer Data to OpenAI for processing involving such Subprocessor. If none of the above options are commercially feasible, in OpenAI's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days of OpenAI's receipt of Customer's objection notice, then either party may terminate any subscriptions, order forms or usage regarding the Services that cannot be provided without the use of the new Subprocessor for cause and in such case, Customer will be refunded any pre-paid fees for the applicable subscriptions, order forms or usage to the extent they cover periods or terms following the date of such termination. Such termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor. OpenAI shall enter into contractual arrangements with each Subprocessor binding them to provide a comparable level of data protection and information security to that provided for herein. Subject to the limitations of liability included in the Agreement, OpenAI agrees to be liable for the acts and omissions of its Subprocessors to the same extent OpenAI would be liable under the terms of the DPA if it performed such acts or omissions itself;

h. upon reasonable request no more than once per year, provide Customer with OpenAI's privacy and security policies and other such information necessary to demonstrate compliance with the obligations set forth in this DPA and applicable Data Protection Laws;

i. where required by law and upon reasonable notice and appropriate confidentiality agreements, cooperate with assessments, audits, or other steps performed by or on behalf of Customer at Customer's sole expense and in a manner that is minimally disruptive to OpenAI's business that are necessary to confirm that OpenAI is processing Customer Data in a manner

consistent with this DPA. Where permitted by law, OpenAI may instead make available to Customer a summary of the results of a third-party audit or certification reports relevant to OpenAI's compliance with this DPA. Such results, and/or the results of any such assessments, audits, or other steps shall be the Confidential Information of OpenAI;

j. to the extent that Customer permits or instructs OpenAI to process Customer Data subject to U.S. Privacy Laws in a de-identified, anonymized, and/or aggregated form as part of the Services, OpenAI shall (i) adopt reasonable measures to prevent such deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) not attempt to re-identify the information, except that OpenAI may attempt to reidentify the information solely for the purpose of determining whether its de-identification processes comply with Data Protection Laws or are functioning as intended; and (iii) before sharing de-identified data with any other party, including Subprocessors, contractually obligate any such recipients to comply with the requirements of this provision;

k. where the Customer Data is subject to the CCPA, not (i) retain, use, disclose, or otherwise process Customer Data except as necessary for the business purposes specified in the Agreement or this DPA; (ii) retain, use, disclose, or otherwise process Customer Data in any manner outside of the direct business relationship between OpenAI and Customer; or (iii) combine any Customer Data with Personal Data that OpenAI receives from or on behalf of any other third party or collects from OpenAI's own interactions with individuals, provided that OpenAI may so combine Customer Data for a purpose permitted under the CCPA if directed to do so by Customer or as otherwise permitted by the CCPA;

l. where required by law, grant Customer the rights to (i) take reasonable and appropriate steps to ensure that OpenAI uses Customer Data in a manner consistent with Data Protection Laws by exercising the audit provisions set forth in this DPA above; and (ii) stop and remediate unauthorized use of Customer Data, for example by requesting that OpenAI provide written confirmation that applicable Customer Data has been deleted.

2. Notice to Customer

OpenAI will inform Customer if OpenAI becomes aware of:

a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless OpenAI is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;

b. any notice, inquiry or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a "Supervisory Authority") with respect to Customer Data; or

c. any complaint or request (in particular, requests for access to, rectification or blocking of Customer Data) received directly from Customer's data subjects. OpenAI will not respond to any such request without Customer's prior written authorization.

3. Assistance to Customer

OpenAI will provide reasonable assistance to Customer regarding:

a. information necessary, taking into account the nature of the processing, to respond to requests received pursuant to Data Protection Laws from Customer's data subjects in respect of access to or the rectification, erasure, restriction, portability, objection, blocking or deletion of Customer Data that OpenAI processes for Customer. In the event that a data subject sends such a request directly to OpenAI, OpenAI will promptly send such request to Customer;

b. the investigation of any breach of OpenAI's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data processed by OpenAI for Customer (a "Personal Data Breach"); and

c. where appropriate, the preparation of data protection impact assessments with respect to the processing of Customer Data by OpenAI and, where necessary, carrying out consultations with any supervisory authority with jurisdiction over such processing.

4. Required Processing

If OpenAI is required by Data Protection Laws to process any Customer Data for a reason other than in connection with the Agreement, OpenAI will inform Customer of this requirement in advance of any such processing, unless legally prohibited.

5. Security

OpenAI will:

a. maintain reasonable and appropriate organizational and technical security measures, including but not limited to those measures described in Exhibit B to this DPA (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption) to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Data and to protect the rights of the subjects of that Customer Data;

b. take appropriate steps to confirm that OpenAI personnel are protecting the security, privacy and confidentiality of Customer Data consistent with the requirements of this DPA; and

c. notify Customer of any Personal Data Breach by OpenAI, its Subprocessors, or any other third parties acting on OpenAI's behalf without undue delay after OpenAI becomes aware of such Personal Data Breach.

6. Obligations of Customer

a. Customer represents, warrants and covenants that it has and shall maintain throughout the term all necessary rights, consents and authorizations to provide the Customer Data to OpenAI and to authorize OpenAI to use, disclose, retain and otherwise process Customer Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to OpenAI.

b. Customer shall comply with all applicable Data Protection Laws.

c. Customer shall reasonably cooperate with OpenAI to assist OpenAI in performing any of its obligations with regard to any requests from Customer's data subjects.

d. Without prejudice to OpenAI's security obligations in Section 5 of this DPA, Customer acknowledges and agrees that it, rather than OpenAI, is responsible for certain configurations and design decisions for the services and that Customer, and not OpenAI, is responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection Laws.

e. Customer shall not provide Customer Data to OpenAI except through agreed mechanisms. For example, Customer shall not include Customer Data other than technical contact information, or in technical support tickets, transmit user Customer Data to OpenAI by email. Without limitation to the foregoing, Customer represents, warrants and covenants that it shall only

transfer Customer Data to OpenAI using secure, reasonable and appropriate mechanisms, to the extent such mechanisms are within Customer's control.

f. Customer shall not take any action that would (i) render the provision of Customer Data to OpenAI a "sale" under U.S. Privacy Laws or a "share" under the CCPA (or equivalent concepts under U.S. Privacy Laws); or (ii) render OpenAI not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws.

7. International Data Transfers

a. OpenAI Ireland Ltd. will process Customer Data provided by Customer that originates in the EEA or Switzerland. To the extent that OpenAI Ireland Ltd transfers Customer Data to other OpenAI affiliates in jurisdictions that do not provide the same level of data protection, it will do so on the basis of intra-group agreements that incorporate appropriate transfer mechanism provisions to protect Customer Data. Such mechanisms may include the Standard Contractual Clauses adopted by the EU Commission on June 4, 2021 (as may be amended, updated or replaced from time to time) ("EU SCCs") or an adequacy decision issued by the European Commission under Article 45 GDPR.

b. OpenAI OpCo, LLC will process Customer Data provided by Customer located in the UK in accordance with the EU SCCs as amended by the UK addendum to the EU SCCs issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018 ("UK Addendum") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows (each as amended by the UK Addendum, where relevant and applicable):

i. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and OpenAI is processing Customer Data as a processor.
ii. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and OpenAI is processing Customer Data as a sub-processor.

c. For each module of the EU SCCs, where applicable, the following applies:

i. The optional docking clause in Clause 7 does not apply;
ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA.
iii. In Clause 11, the optional language does not apply;
iv. All square brackets in Clause 13 are hereby removed;
v. In Clause 17 (Option 1), the EU SCCs will be governed by the laws of England and Wales;
vi. In Clause 18(b), disputes will be resolved before the courts of England and Wales;
vii. Exhibit A to this DPA contains the information required in Annex I and Annex III of the EU SCCs;
viii. Exhibit B to this DPA contains the information required in Annex II of the EU SCCs; and

d. The parties will comply with the terms of Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B1.0 . The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Exhibit A to this DPA and (ii) that either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

8. Term; Data Return and Deletion

This DPA shall remain in effect as long as OpenAI carries out Customer Data processing operations on Customer's behalf or until the termination of the Agreement (and all Customer Data has been returned or deleted in accordance with this DPA). OpenAI will retain API Service Customer Data sent through the API for a maximum of thirty (30) days, after which it will be deleted, except where OpenAI

is required to retain copies under applicable laws, in which case OpenAI will isolate and protect that Customer Data from any further processing except to the extent required by applicable laws. OpenAI will retain ChatGPT Enterprise Service Customer Data during the term of the Agreement, unless otherwise stated in the Agreement or Order Form. On the termination of the DPA, OpenAI will direct each Subprocessor to delete the Customer Data within thirty (30) days of the DPA's termination, unless prohibited by law. For clarity, OpenAI may continue to process information derived from Customer Data that has been deidentified, anonymized, and/or aggregated such that the data is no longer considered Personal Data under applicable Data Protection Laws and in a manner that does not identify individuals or Customer to improve OpenAI's systems and services.

OpenAI, LLC	**Trustees of the California State University**
Signature: Aliisa Rosenthal Aliisa Rosenthal (Jan 17, 2025 16:41 PST)	Signature: David Beaver
Name: Aliisa Rosenthal	Name: David Beaver
Title: Head of Enterprise	Title: Chief Procurement Officer
Date: Jan 17, 2025	Date: Jan 17, 2025

Exhibit A

A. LIST OF PARTIES

Data exporter(s): the Services customer identified on the applicable Services registration documents

Data importer(s):

Name: OpenAI OpCo, LLC

Address: 1455 Third Street, San Francisco, CA 94158

Contact Person's name, position and contact details:

Emma Redmond
Head of EU Data Protection
privacy@openai.com

Activities relevant to the data transferred under these Clauses: The performance of the services described in the agreement to which this is attached.

Signature and date: Emma Redmond 1/24/2024

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of data exporters applications.

Categories of personal data transferred

Name, contact information, demographic information, or other information provided by the user in unstructured data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data is intended to be transferred unless the user includes it unexpectedly in unstructured data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

The performance of the services described in the agreement to which this exhibit is attached.

Purpose(s) of the data transfer and further processing

The performance of the services described in the agreement to which this exhibit is attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

During the term of the agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The performance of the services described in the agreement to which this exhibit is attached.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Information Commissioner's Office ("ICO").

Exhibit B

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

INTRODUCTION

OpenAI's mission is to deploy safe and responsible AI at scale for the benefit of all. In accordance with this mission, OpenAI maintains an information security program designed to safeguard its systems, data, and Customer Data. This Exhibit describes the information security program and security standards that OpenAI maintains with respect to the Services and handling of data submitted by or on behalf of Customer of the Services (the "Customer Data"). Capitalized terms not defined in this Exhibit have the meanings given in the DPA or Agreement.

ChatGPT Enterprise is a new OpenAI Service and so certain technical or security measures below apply differently to ChatGPT Enterprise; in each case that difference is noted in *italicized* language. "ChatGPT Enterprise" is the version of OpenAI's AI-powered ChatGPT language model that is available to enterprises.

To learn more about OpenAI's technical and organizational security measures to protect Customer Data, see the OpenAI Trust Portal at https://trust.openai.com/ (the "Trust Portal"). The Security Measures below include the subset of the information available in the Trust Portal which applies to this DPA.

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- OpenAI uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services;
- Mandatory multi-factor authentication is used for authenticating to OpenAI's identity provider.
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning OpenAI does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.
- Cloud Infrastructure and Network Security. OpenAI maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:
- Separate production and non-production environments;

- Primary backend resources are deployed behind a VPN.
- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

System and Workstation Control. OpenAI maintains industry best practices for securing OpenAI's corporate systems, including laptops and on-premises infrastructure, including:

- Endpoint management of corporate workstations;
- Endpoint management of mobile devices;
- Automatic application of security configurations to workstations;
- Mandatory patch management; and
- Maintaining appropriate security logs.

Data Access Control. OpenAI maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Disclosure Control. OpenAI maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;
- Encryption of data in transit;
- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations;
- Restrictions on use of portable or removable media; and
- Customer Data can be deleted upon request.

Availability control. OpenAI maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.

Segregation control. OpenAI maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities;

- Segregation of business information system functions; and
- Segregation of testing and production information system environments.

Risk Management. OpenAI maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation;
- Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk. Upon request, OpenAI will provide summary details of the tests performed and whether the identified issues have been resolved;
- Annual engagements of a qualified, independent external auditor to conduct periodic reviews of OpenAI's security practices against recognized audit standards, including SOC 2 Type II certification audits. Upon reasonable request, OpenAI will provide summary details; and
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

Personnel. OpenAI maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services;
- Annual security training for employees, and supplemental security training as appropriate.

Physical Access Control. OpenAI maintains industry best practices for preventing unauthorized physical access to OpenAI facilities, including:

- Physical barrier controls including locked doors and gates;
- 24-hour on-site security guard staffing;
- 24-hour video surveillance and alarm systems, including video surveillance of common areas and facility entrance and exit points;
- Access control systems requiring biometrics or photo-ID badge and PIN for entry to all OpenAI facilities by OpenAI personnel;
- Visitor identification,sign-in and escort protocols; and
- Logging of facility exits and entries.

Third Party Risk Management. OpenAI maintains industry best practices for managing third party security risks, including with respect to any subprocessor or subcontractor to whom OpenAI provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by OpenAI's Security team.

Security Incident Response. OpenAI maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- OpenAI aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If OpenAI becomes aware that a Personal Data Breach has occurred, OpenAI will notify Customer in accordance with the DPA.

Security Evaluations. OpenAI performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of OpenAI's information systems.

OPENAI ORDER FORM

Offer Valid Until: January 31, 2025

OpenAI, L.L.C. ("OpenAI")
548 Market Street
PMB 97273
San Francisco, California 94104-5401
United States

BILLING INFORMATION

Bill to: Trustees of the California State University

Ship to: 401 Golden Shore, Long Beach, California 90802, United States

Billing contact: accountspayable@calstate.edu

Primary contact: mtrullinger@calstate.edu

CHATGPT SERVICES

Term	Service	Quantity (users)	Start Date	End Date	Net Total
Term 1	ChatGPT Education	40,000	January 1, 2025	June 30, 2025	$1,920,000.00
Term 2	ChatGPT Education	500,000	July 1, 2025	June 30, 2026	$15,000,000.00
				Net Amount	$16,920,000.00
Term 1				Free Monthly API Credit	$1,500.00
Term 2				Free Monthly API Credit	$3,000.00

CHATGPT ADDITIONAL TERMS

- **Service**. Customer is purchasing the services listed above. For the duration of Term 1 and Term 2, Customer's ChatGPT Education licenses will, at a minimum, include all features and functionality listed in Exhibit A, or the reasonable equivalent made generally available to other ChatGPT Education customers.

- **Billing Schedule**. Customer will be invoiced as follows:
  Term 1: Effective date of the Agreement
  Term 2: July 1, 2025

- **Additional End Users**. Customer may not increase the number of End Users (the "Additional End Users") during Term 2 unless mutually agreed upon through an Order Form. At OpenAI's discretion, Customer may receive access to the service prior to the Start Date, without payment of additional fees, subject to the terms and conditions of this Agreement.

- **End User Upgrades**. Customer may choose to upgrade select End Users to standard ChatGPT Edu offering at a cost of an additional $5.50 per user/month through the execution of an additional Order Form through its designated Administrator(s) during the Term of the contract.

- **Enterprise API**. Customer is granted monthly API credits as listed above. Additional use of the API, if any, is subject to the Agreement and the pricing set forth at https://openai.com/pricing. API usage is invoiced on a monthly basis in arrears according to the Payment Information below.

PAYMENT TERMS

Payment Term:	Net 30	**PO required?**	Yes
Currency:	USD	**PO Number:**	
Payment Method:	ACH	**VAT/GST number:**	N/A

ORDER FORM TERMS

- **Customer Agreement**. Customer's use of OpenAI Services is subject to the Enterprise Agreement between the parties executed on or about the Effective Date (together with this Order Form, the "**Agreement**").
- **Publicity.** Subject to Customer's prior written consent in each case (which for clarity is not provided in this Order Form), OpenAI may use Customer's name, logo and marks to identify Customer in marketing materials and on OpenAI's website, solely in accordance with brand guidelines that Customer makes available to OpenAI. In addition, subject to Customer's prior written consent, OpenAI may produce and publish a case study regarding Customer's use of the Services.
- **No Auto-Renewal**. At the end of the Term, this Order Form will not renew. Access to the Services will expire as described in the Agreement, unless otherwise agreed in writing by the Parties. If Customer and OpenAI elect to renew under this Agreement and the Customer reduces its license count, quantity, or minimum commitment by no more than fifty percent (50%) OpenAI will not adjust or remove discounts offered to Customer based on its prior purchase, maintaining the same per license fee as Term 2.
- **Start Date**. If this Order Form is executed after the applicable Start Date for the Services set forth on this Order Form, OpenAI may adjust the Start Date, without increasing the Fees, based on the date OpenAI activates the services, provided that the total term length does not change.

[Signatures to follow]

Accepted and Agreed:

OpenAI, L.L.C.

Signature: Aliisa Rosenthal
Aliisa Rosenthal (Jan 17, 2025 16:41 PST)

Name: Aliisa Rosenthal

Title: Head of Enterprise

Date: Jan 17, 2025

Trustees of the California State University

Signature: David Beaver

Name: David Beaver]

Title: Chief Procurement Officer

Date Jan 17, 2025

Exhibit A

Category	Features
Essentials	
Messages and interactions	Unlimited
Chat history	Unlimited
Access on web, iOS, Android	☑
Model Quality	
GPT-4o access	10 messages/5hr
4o-mini	Unlimited
Context window	32K
Regular quality & speed updates as models improve	☑
Functions	
Browse	☑
Data analysis	☑
Vision	☑
File uploads	☑
Discover & use GPTs	☑
Create & share GPTs	☑
Share GPTs with your workspace	☑
Image generation	☑
Privacy	
Content is used to train our models	No
Custom data retention windows	☑
Security & Administration	
Dedicated workspace	☑
Unified billing	☑
GPTs analytics and management	☑
Admin console	☑
Bulk member management	☑
Admin roles	☑
Soc 2 Type 2 compliance	☑
SAML SSO	☑
Domain verification	☑
Granular GPT controls & group permissions	☑
Analytics dashboard	☑
Compliance API	☑