OPENAI ENTERPRISE AGREEMENT

This Enterprise Agreement is entered into as of the last date set forth on the signature page below ("**Effective Date**") between OpenAI, L.L.C. ("**OpenAI**" or "**Supplier**") and The Regents of the University of California ("**Customer, and or UC**"). This Agreement also refers to and incorporates the OpenAI Policies (defined below) and any ordering document signed by Customer and OpenAI or OpenAI webpage that Customer uses to purchase the Services (an "**Order Form**") (collectively, the "**Agreement**"). Capitalized terms not defined in this Agreement will have the meaning set forth in the Order Form.

1. General.

1.1 The Services (defined below) are covered by the UC Purchase Order ("PO") and/or other written agreement of the Parties (defined below), (which, when combined with this Enterprise Agreement and any other documents incorporated by reference, will constitute the "Agreement") and are governed by the Agreement. As used herein, "UC" refers to The Regents of the University of California, a corporation described in California Constitution Art. IX, Sec. 9, on behalf of the UC Locations identified in the Agreement, the Order Form and/or the PO. UC and Supplier individually will be referred to as "Party" and collectively as "Parties." Any defined terms not defined herein will have the meaning ascribed to such term in any of the other documents incorporated in and constituting the Agreement. No other terms or conditions will be binding upon the Parties unless accepted by them in writing. Supplier accepts all of the Agreement's terms and conditions either in writing, by shipping any portion of the Goods, or performing any portion of the Services. The terms of any proposal referred to in the Agreement are included and made a part of the Agreement only to the extent the proposal is executed in writing by the Parties, specifies the Services ordered, the price therefor, and the delivery thereof, and then only to the extent that such terms are consistent with the terms and conditions of the Agreement unless otherwise expressly set forth therein.

For purposes of this Agreement, a UC Location shall include but not be limited to all current and future UC Locations of the University of California and its Affiliates as further detailed at https://www.universityofcalifornia.edu/uc-system/parts-of-uc.

2. Services.

2.1 *Use of Services*. OpenAI grants Customer a non-exclusive right to access and use the Services during the Term (as defined below). This includes the right to use OpenAI's application programming interface ("**API**") to integrate the Services into Customer's applications, products, or services (each a "**Customer Application**") and to make Customer Applications available to End Users (as defined below). "**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 Offering.

2.2 *Third-Party Offering*. Third parties may offer products, services, or content through the Services ("**Third Party Offering**"). If Customer elects, in its sole discretion, to access or use a Third Party Offering (including by making it available via a Customer Application), Customer's access and use of the Third Party Offering is subject to this Agreement and any additional terms applicable to the Third Party Offering.

2.3 *Responsibilities for Customer's Account*. Customer must provide accurate and up-to-date account information. Customer is responsible for all activities that occur under Customer's account, including the activities of any end user (each, an "**End User**") who is provisioned with an account under Customer's account (an "**End User Account**") or accesses the Services through a Customer Application. Customer may not make account access credentials available to third parties or share individual login credentials between multiple users on an account. Customer may not resell or lease access to its account or any End User Account. Customer will promptly notify OpenAI if Customer becomes aware of any unauthorized access to or use of Customer's account or the Services.

2.4 *Customer Affiliates*. Customer's Affiliates may enter Order Forms under this Agreement, in which case, such Affiliates will be bound by the terms of this Agreement as if they were a signatory hereto. Customer will be responsible and liable for all acts and omissions of its Affiliates that access the Services under this Agreement as if such acts or omissions were undertaken by the Customer itself. "**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.

3. Restrictions. OpenAI owns all right, title, and interest in and to the Services. Customer only receives rights to use the Services as explicitly granted in this Agreement. Customer will not and will not permit End Users to (except for UC student End Users for whom Customer's obligation under this Section 3 is to instruct and require such student End Users to accept Customer end user terms that include the following restrictions):

a. use the Services or Customer Content (as defined below) in a manner that violates any applicable laws or OpenAI's Service Terms (available at https://openai.com/policies/service-terms), Sharing & Publication Policy (available at https://openai.com/policies/sharing-publication-policy), and Usage Policies (available at https://openai.com/policies/usage-policies), and any other guidelines or policies OpenAI provides in writing (the "**OpenAI Policies**");

b. use the Services or Customer Content in a manner that infringes, misappropriates, or otherwise violates any third party's rights;

c. send OpenAI any personal information of children under 13 or the applicable age of digital consent or allow minors to use OpenAI Services without consent from their parent or guardian;

d. 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);

e. use Output (as defined below) to develop any artificial intelligence models that compete with OpenAI's products and services. However, Customer can use Output to (i) develop artificial intelligence models primarily intended to categorize, classify, or organize data (e.g., embeddings or classifiers), as long as such models are not distributed or made commercially available to third parties and (ii) fine tune models provided as part of the Services.

f. use any method to extract data from the Services other than as permitted through the API; or

g. buy, sell, or transfer API keys from, to or with a third party.

4. Assigned Personnel, Character of Service. Supplier will provide the Services as an independent contractor and furnish all equipment, personnel, and supplies sufficient to provide the Services expeditiously and efficiently as set forth herein, and at such locations as UC may so require and as agreed to in writing by the Parties in any Order Form. Supplier will devote industry standard qualified personnel to perform the Services under the Agreement. At no time will Supplier or Supplier's employees, sub-suppliers, agents, or assigns be considered employees of UC for any purpose, including but not limited to workers' compensation provisions. Supplier shall not have the power nor right to bind or obligate UC, and Supplier shall not hold itself out as having such authority. Supplier shall be responsible to UC for all Services performed by Supplier's employees, agents and subcontractors under this Agreement, including being responsible for ensuring payment of all unemployment, social security, payroll, contributions and other taxes with respect to such employees, agents and subcontractors.

5. Content.

5.1 *Customer Content*. Customer and Customer's End Users may provide input to the Services ("**Input**"), and receive output from the Services based on the Input ("**Output**"). Input and Output together are "**Customer Content**." As between Customer and OpenAI, and to the extent permitted by applicable law, Customer (a) retains all ownership rights in Input and (b) owns all Output. OpenAI hereby assign to Customer all OpenAI's right, title, and interest, if any, in and to Output.

5.2 *OpenAI Obligations for Customer Content*. OpenAI will process and store Customer Content in accordance with OpenAI's Enterprise privacy page located at https://openai.com/enterprise-privacy. OpenAI will only use

Customer Content as necessary to provide Customer with the Services, comply with applicable law, and enforce OpenAI Policies. OpenAI will not use Customer Content to develop or improve the Services.

5.3 *Customer Obligations for Customer Content*. Customer is responsible for all Input and represents and warrants that Customer 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, including by utilizing human review as appropriate.

5.4 *Similarity of Output*. Customer acknowledges that 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 Output.

6. Confidentiality.

6.1 *Use and Nondisclosure*. "**Confidential Information**" means any business, technical or financial information, materials, or other subject matter disclosed by one party ("**Discloser**") to the other party ("**Recipient**") under this Agreement that is identified as confidential at the time of disclosure or should be reasonably understood by Recipient to be confidential under the circumstances. For the avoidance of doubt, Confidential Information includes Customer Content. Any information derived from Confidential Information shall also be considered Confidential Information (except, for clarity, analytics or other data generated in connection with Customer's use of the Services which do not include Confidential Information (e.g. if Customer Content triggers a safety classifier pre-defined by OpenAI as a possible violation of OpenAI policy, neither that safety classifier nor the fact that such classifier was triggered are considered Confidential Information). Recipient agrees it will: (a) only use Discloser's Confidential Information to exercise its rights and fulfill its obligations under this Agreement (including for safety features within the Services), (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.

6.2 *Exceptions*. The obligations in Section 6.1 do not apply to any 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 lawful 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. Recipient may disclose Confidential Information only to its employees, contractors, and agents (including, for OpenAI, its subprocessors which OpenAI uses to provide the Services) who have a need to know and who are bound by confidentiality obligations at least as restrictive as those of this Agreement. Recipient will be responsible for any breach of this Section 6 by its employees, contractors, and agents. Except as expressly set forth in this Section 6, Recipient may only disclose Confidential Information as provided in Section 21.

7. Security.

7.1 *OpenAI's Security Program*. OpenAI will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) protect the Services and Customer Content against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access, and (c) minimize security risks, including through regular risk assessments and testing.

7.2 *OpenAI's Security Obligations*. As part of OpenAI's information security program, OpenAI will: (a) implement and enforce policies related to electronic, network, and physical monitoring and data storage, transfer, and access; (b) deploy production infrastructure behind VPNs where possible; (c) require multi-factor authentication for employees; (d) configure network security, firewalls, accounts, and resources for least-privilege access; (e) maintain a logging and incident response process; (f) maintain corrective action plans to respond to potential security threats; and (g) conduct periodic reviews of OpenAI security and the adequacy of OpenAI's information security program as aligned to industry best practices and OpenAI's own policies and procedures.

8. Privacy.

8.1 *Personal Data*. If Customer uses the Services to process personal data, Customer must (a) provide legally adequate privacy notices and obtain necessary consents for the processing of personal data by the Services, (b) process personal data in accordance with applicable law, and (c) if processing "personal data" or "Personal Information" as defined under applicable data protection laws, execute OpenAI's Data Processing Addendum ("**DPA**").

8.2 *HIPAA*. Customer agrees not to use the Services to create, receive, maintain, transmit, or otherwise process any information that includes or constitutes "Protected Health Information", as defined under the HIPAA Privacy Rule (45 C.F.R. Section 160.103), unless Customer has signed a Healthcare Addendum and Business Associate Agreement (together, the "**Healthcare Addendum**") with OpenAI prior to creating, receiving, maintaining, transmitting, or otherwise processing this information.

9. Payment; Taxes.

9.1 Pricing is set forth in the Agreement and the applicable Order Form or PO, and the amount UC is charged and responsible for shall not exceed the amount specified in the Agreement unless UC has given prior written approval. Supplier will submit invoices following the designated invoice method directly to UC Accounts Payable Departments at each UC Location, unless UC notifies the Supplier otherwise by amendment to the Agreement. UC will pay Supplier, upon submission of undisputed invoices, for Services provided under the Agreement in accordance with the applicable Order Form. Invoices must reference the Agreement or PO number. Any of Supplier's expenses that UC agrees to reimburse will be reimbursed under UC's Travel Policy, which may be found at http://www.ucop.edu/central-travel-management/resources/index.html. Where applicable and except as set forth in Section 9.2 below, Supplier will pay all taxes imposed on Supplier in connection with its performance under the Agreement, including any federal, state and local income, sales, use, excise and other taxes or assessments. Notwithstanding any other provision to the contrary, UC will not be responsible for any fees, interest or surcharges Supplier wishes to impose other than the finance charge for late payment as set forth below. Fees are payable in U.S. dollars and are nonrefundable except as provided in this Agreement.

9.2 *Taxes*. Fees are exclusive of taxes, which OpenAI will charge as required by applicable law in connection with the Services. OpenAI will use the name and address in Customer's account as the place of supply for tax purposes.

9.3 To dispute an invoice, Customer must contact ar@openai.com within sixty (60) days of issuance. OpenAI may suspend the Services within 10 days after providing written notice of late payment for overdue undisputed amounts.

10. Term; Termination.

10.1 *Term*. The term of this Agreement will commence upon the final signature date below (" Effective Date"). The initial term of the Agreement will be for three (3) years after the Effective Date (Initial Term). UC may renew the Agreement for three (3) successive one (1) year periods (each, a Renewal Term), by providing OpenAI with at least 30 calendar days' written notice before the end of the Initial Term or any Renewal Term. Any active Order Forms referencing this Agreement at termination will expire or terminate in accordance with the term of the Order Form and remain subject to the terms of the Agreement until such expiration or termination.

10.2 UC's obligation to proceed is conditioned upon the appropriation of state, federal and other sources of funds not controlled by UC ("Funding"). UC will have the right to terminate the Agreement without damage, penalty, cost or further obligation in the event that through no action or inaction on the part of UC, the Funding is withdrawn; provided, however, that any existing Order Form in effect will continue until the expiration or termination of the term of such Order Form.

10.3 Both Customer and OpenAI may terminate this Agreement upon written notice (a) if the other party materially breaches this Agreement and does not cure the breach within thirty (30) days after receiving written notice of the breach or (b) if the other party ceases its business operations or becomes subject to insolvency proceedings. OpenAI may suspend Customer or any End User's access to the Services or terminate this Agreement or any Order Form: (i) if required to do so by law; (ii) to prevent a security risk or other credible risk of harm or liability to us, the Services, or any third party; or (iii) for repeated or material violations of the OpenAI Policies or in the case of UC student End Users any violations of Sections 3(a)-(g). OpenAI will use reasonable efforts to notify Customer of any suspension or termination and give Customer the opportunity to resolve the issue prior to suspension or termination.

10.4 *Effect of Termination*. 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 or expiration. Upon termination or expiration of this Agreement, the provisions that are intended by their nature to survive termination will survive and continue in full force and effect in accordance with their terms, including confidentiality obligations, limitations of liability, and disclaimers. Upon termination of this Agreement, OpenAI will delete all Customer Content from its systems within 30 days, unless OpenAI is legally required to retain it.

11. Warranties; Disclaimer.

Supplier makes the following warranties. Supplier acknowledges that failure to comply with any of the warranties in the Agreement will constitute a material breach of the Agreement, and UC will have the right to terminate the Agreement in accordance with Section 10 above without damage, penalty, cost or further obligation other than payment obligations for Services performed prior to the effective date of termination.

a. General Warranties. Supplier represents, warrants and covenants that: (i) Supplier has the right to enter into this Agreement; (ii) Supplier will comply with all applicable laws, rules and regulations in performing Supplier's obligations hereunder; (iii) the Services shall be performed in a professional manner by competent personnel, in accordance with the prevailing industry standards; (iv) the Services will conform in all material respects with the specifications provided by OpenAI, including in OpenAI documentation, and v) If Supplier makes generally available additional warranties to its customers (e.g. pursuant to Supplier's online terms located at openai/policies/business-terms/). Supplier agrees to offer the same or substantially similar warranties to the UC upon UC's notice to Supplier, and the parties agree to negotiate in good faith to amend the terms of this Agreement to incorporate such additional warranties. The rights and remedies so provided are in addition to and do not limit any rights afforded to UC by any other article of the Agreement.

b. Permits and Licenses. Supplier agrees to procure all necessary permits or licenses required by the state, territory and political subdivision or any other country in which the Services are provided in order to provide the Services hereunder.

c. Accessibility Requirements. As applicable to the Supplies and/or Services being provided under the Agreement, Supplier will comply with the Accessibility Commitments set forth on Exhibit A.

d. California Child Abuse and Neglect Reporting Act ("CANRA"). If applicable to Supplier's performance of the Services hereunder, Supplier warrants that it complies with CANRA.

e. Debarment, Suspension, U.S. Government Restricted Party Lists. Supplier warrants that it is not on the U.S. government's Denied Parties List, the Unverified List, the Entities List, the Specially Designated Nationals and Blocked Parties List, and is not presently as of the Effective Date debarred, suspended, proposed for debarment or otherwise declared ineligible for award of federal contracts or participation in federal assistance programs or activities.

f. UC Trademark Licensing Code of Conduct. If the Services provided to UC under this Agreement will bear UC's name (including UC campus names, abbreviations of these names, UC logos, UC mascots, or UC seals) or other trademarks owned by UC, Supplier warrants that it h olds a valid license (to the extent applicable) from UC and complies with the Trademark Licensing Code of Conduct policy, available at http://policy.ucop.edu/doc/3000130/TrademarkLicensing.

g. Outsourcing (Public Contract Code section 12147) Compliance. Supplier warrants that it will not subcontract its obligations under the Agreement to subprocessors outside the United States, except as described

in Supplier's bid or the DPA. If Supplier or its sub-supplier performs the Agreement with subprocessors outside the United States during the term of the Agreement and Supplier did not describe such work in its bid or the DPA, Supplier acknowledges and agrees that UC may terminate the Agreement upon written notice without further obligation for noncompliance in accordance with the DPA. In such event, if required under applicable law and to the extent that the parties are able to quantify the amount, Supplier will forfeit to UC (by way of a credit, as permitted by applicable law and UC policy) the amount UC paid for the percentage of work that was performed with subprocessors outside the United States and not described in Supplier's bid or DPA.

12. Indemnification and Limitation of Liability.

12.1 Supplier's Indemnity. To the fullest extent permitted by law, Supplier will defend, indemnify, and hold harmless UC, its officers, employees, agents, affiliates and licensors from and against all losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities of any kind resulting from or arising out of any third party claims (i) alleging that the Services (including training data OpenAI uses to train a model that powers the Services) infringe any third party intellectual property right; (ii) arising out of the gross negligence or willful misconduct of Supplier under the Agreement, including the performance hereunder of Supplier, its officers, employees, agents, sub-suppliers, or anyone directly or indirectly employed by Supplier, or any person or persons under Supplier's direction and control, provided such losses, expenses, damages and liabilities are due or claimed to be due to the acts or omissions of Supplier, its officers, employees, agents, sub-suppliers, or anyone directly or indirectly employed by Supplier, or any person or persons under Supplier's direction and control; and (iii) in connection with Security Breach Costs as defined in Section 12.3 arising from Supplier or its subprocessors performance of its obligations under this Agreement. In connection with the indemnity in subsection (i) above, this excludes claims to the extent caused by: (a) fine-tuning, customization, or modification of the Services by any party other than OpenAI or its agents (including sub-processors) to the extent such claim would not have occurred without such finetuning, customization, or modification, (b) combination of any Services with products, services, or software not provided by OpenAI or on OpenAI's behalf, to the extent such claim would not have occurred without such combination, (c) Customer's failure to comply with this Agreement or laws, regulations, or industry standards applicable to Customer, or (d) Customer Applications (if any and the claim would not have arisen but for the Customer Application. UC agrees to provide Supplier with prompt written notice of any such claim or action and to permit Supplier to defend any claim or action, and that UC will cooperate fully in such defense. UC retains the right to participate in the defense against any such claim or action at its sole cost and expense, and the right to consent to any settlement requiring UC to admit liability, which consent will not unreasonably be withheld or delayed.

12.2 UC's Indemnity. To the fullest extent permitted by law, UC will defend, indemnify, and hold harmless Supplier, its officers, employees, agents, affiliates and licensors from and against all losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities of any kind resulting from or arising out of (i) use of the Services in violation of this Agreement (including violation of OpenAI policies); and(ii) any third party claim relating Customer Applications (if any), Input, or Institutional Information, but only to the extent caused by the acts and omissions of UC, its officers, employees, or agents. Supplier agrees to provide UC with prompt written notice of any such claim or action and to permit UC to defend any claim or action, and that Supplier will cooperate fully in such defense. Supplier retains the right to participate in the defense against any such claim or action at its sole cost and expense, and the right to consent to any settlement requiring Supplier to admit liability, which consent will not unreasonably be withheld or delayed.

12.3 ***Limitation on Indirect Liability. Except for (i) a party's gross negligence or willful misconduct, (ii) Customer's breach of Section 3 (Restrictions), (iii) either party's breach of confidentiality , (iv) OpenAI's breach of Section 7, (v) breach of Section 2 (Obligations of the Parties) of the Healthcare Addendum; (vi) Security Breach Costs arising from Supplier or its subprocessors performance of its obligations under this Agreement, or (vii) indemnification required under Sections 12.1 and 12.2, 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 that party has been advised of the possibility of those damages.***

"Security Breach Costs" consist of costs in connection with a Breach (as defined in the UC Appendix Data Security) of Institutional Information of (a) operating a toll -free telephone call center to handle inquiries, (b) notifications to individuals impacted by such Breach, (c) credit monitoring for such impacted individuals, (d) civil fines or penalties, (e) engaging information technology consultants to reasonably assist with any mitigation and remediation of such Breach, (f) third party claims arising from such Breach, including reasonable litigation and settlement costs, subject to the indemnity process set forth in Section 12.1, (g) in connection with Customer's use of the API, any payment made to a third party as a result of extortion (i.e., ransom payment following ransomware) related to such Breach.

12.4 ***Liability Cap. Except for (i) a party's gross negligence or willful misconduct, (ii) Customer's breach of Section 3 (Restrictions), (iii) either party's breach of confidentiality, (iv) OpenAI's breach of Section 7, (v) breach of Section 2 (Obligations of the Parties) of the Healthcare Addendum, (vi) Security Breach Costs arising from Supplier or its subprocessors performance of its obligations under this Agreement, or (vii) indemnification required under Sections 12.1 and 12.2, each party's total liability under the Agreement will not exceed the total amount Customer has paid to OpenAI in the twelve (12) months immediately prior to the event giving rise to liability. Notwithstanding the foregoing, (a) Supplier's maximum aggregate liability for Security Breach Costs arising from Supplier or its subprocessors performance of its obligations under this Agreement and OpenAI's indemnity in Section 12.1(iii) above, and (b) each party's maximum aggregate liability for breach of Section 2 (Obligations of the Parties) of the Healthcare Addendum, shall not exceed the greater of five (5) times the total amount Customer has paid to OpenAI in the twelve (12) months immediately prior to the event giving rise to liability or five (5) million dollars .***

13. Export Controls***.***

13.1 Customer may not use the Services in or for the benefit of, or export or re-export countries subject to comprehensive sanctions under § 746.1(a) of the Export Administration Regulations (15 CFR chapter VII, subchapter C), or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals, the U.S. Department of Commerce Denied Persons List or Entity List, or any other restricted party lists published by the Office of Foreign Asset Control listing individuals and entities denied export privileges (collectively, "**Restricted Party Lists**", except as authorized under applicable U.S. export control law pursuant to a general or specific license, license exception or exclusion). Customer represents and warrants that except as authorized by applicable U.S. export control law, that Customer and End Users are not located in any U.S. embargoed countries and are not on any Restricted Party Lists and that Customer will comply with all applicable laws related to export controls.

13.2 Supplier agrees to provide UC (the contact listed on the PO) with written notification that identifies the export-controlled Goods or Services and the export classification of such Goods or Services if any of the Goods or Services provided to UC is export-controlled under the International Traffic in Arms Regulations (ITAR) (22 CFR §§ 120-130), the Export Administration Regulations (15 CFR §§ 730 – 734) 500 0r 600 series, or controlled on a U.S. military strategic goods list. Supplier agrees to provide UC (the contact listed on the PO) with written notification if Supplier will be providing information necessary for the operation, installation, maintenance (checking), repair, overhaul, and refurbishing of Goods that is beyond a standard user manual (i.e., "Use" technology as defined under the EAR 15 CFR §772.1, or "Technical Data" (as defined under the ITAR 22 CFR § 120.10). OpenAI does not provide export-controlled Goods or Services, or related Technical Data.

14. Use of UC Name and Trademark.

14.1 Supplier will not use the UC name, abbreviation of the UC name, trade names and/or trademarks (i.e., logos and seals) or any derivation thereof, in any form or manner in advertisements, reports, or other information released to the public in connection with this Agreement, or place the UC name, abbreviations, trade names and/or trademarks or any derivation thereof on any consumer goods, products, or services for sale or distribution to the

public in connection with this Agreement, without UC's prior written approval. If applicable, Supplier agrees to comply at all times with California Education Code Section 92000.

15. Intellectual Property, Copyright, Patents, and Data Rights

a. General. Should the Services become, or in Supplier's opinion be likely to become, the subject of a claim of infringement of any patent, copyright, trademark, trade name, trade secret, or other proprietary right of any third party, Supplier will provide written notice to UC of the circumstances giving rise to such claim or likely claim. In the event that UC receives notice of a claim of infringement or is made a party to or is threatened with being made a party to any claim of infringement related to the Services, UC will provide Supplier with written notice of such claim or threat. Following receipt of such notice, Supplier will either (at Supplier's sole election) (i) procure for UC the right to continue to use the affected portion of the Services in accordance with this Agreement, or (ii) replace or otherwise modify the affected portion of the Services to make them non-infringing, or obtain a reasonable substitute product for the affected portion of the Services, provided that any replacement, modification or substitution under this paragraph does not effect a material diminishment in the Services' functionality. If none of the foregoing options is reasonably acceptable to UC, UC or Supplier will have the right to terminate the Agreement without damage, penalty, cost or further obligation, and Supplier will refund any prepaid amounts for unused Services. UC will promptly comply with all reasonable instructions provided by Supplier, including any instruction to replace, modify, or cease use of an impacted Service.

b. UC Rights to Institutional Information. Institutional Information shall belong exclusively to UC and unless expressly provided, this Agreement shall not be construed as conferring on Supplier any patent, copyright, trademark, license right or trade secret owned or obtained by UC. Any right for Supplier to use Institutional Information is solely provided on a non-exclusive basis, and only to the extent required for Supplier to provide the Services under the Agreement, comply with applicable law, and enforce OpenAI Policies.

16. Insurance.

a. Supplier, at its sole cost and expense, will insure its activities in connection with providing the Services and obtain, keep in force, and maintain the insurance with the minimum limits as follows. (a) Workers Compensation with statutory limits and Employers Liability with a minimum limit of $1,000,000, (b) Commercial General Liability with a minimum limit of $2,000,000 per occurrence and $4,000,000 in the aggregate and (c) Technology Errors & Omissions Liability and Cyber/Privacy Liability coverage with a minimum of $5,000,000 per occurrence/claim and in the aggregate, such coverage will include without limitation: Costs to notify parties whose data were lost or compromised; Costs to provide credit monitoring and credit restoration services to parties whose data were lost or compromised; Costs associated with third party claims arising from the confirmed or suspected Breach of Institutional Information or loss of Institutional Information, including litigation costs and settlement costs; Any investigation, enforcement, fines and penalties, or similar miscellaneous costs; and any payment made to a third party as a result of extortion related to a confirmed or suspected Breach of Institutional Information. Supplier will provide UC with Supplier's certificate of insurance upon UC's request.

17. Federal Funds.

A. For commercial transactions involving funds on a federal contract (federal awards governed by the FAR), UC will notify OpenAI in the applicable Order Form of any such transactions, and the following provisions will apply to such Order Form, as applicable:

a. FAR 52.203-13, Contractor Code of Business Ethics and Conduct;
b. FAR 52.203-17, Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights;
c. FAR 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements;
d. FAR 52.219-8, Utilization of Small Business Concerns;
e. FAR 52.222-17, Non-displacement of Qualified Workers;
f. FAR 52.222-21, Prohibition of Segregated Facilities;
g. FAR 52.222-26, Equal Opportunity;

h. FAR 52.222-35, Equal Opportunity for Veterans;
i. FAR 52.222-36, Equal Opportunity for Workers with Disabilities;
j. FAR 52.222-37, Employment Reports on Veterans;
k. FAR 52.222-40, Notification of Employee Rights Under the National Labor Relations Act;
l. FAR 52.222-41, Service Contract Labor Standards;
m. FAR 52.222-50, Combating Trafficking in Persons;
n. FAR 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment - Requirements;
o. FAR 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services - Requirements;
p. FAR 52.222-54, Employment Eligibility Verification;
q. FAR 52.222-55, Minimum Wages Under Executive Order 13658;
r. FAR 52.222-62, Paid Sick Leave under Executive Order 13706;
s. FAR 52.224-3, Privacy Training;
t. FAR 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations;
u. FAR 52.233-1, Disputes; and
v. FAR 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels.

B. For non-commercial transactions involving funds on a federal contract, the UC Appendix titled 'Federal Government Contracts Special terms and Conditions (Non-Commercial Items or Services)' and located at www.ucop.edu/procurement- services/policies-forms/index.html is hereby incorporated herein by this reference.

C. For transactions involving funds on a federal grant or cooperative agreement (federal awards governed by CFR Title 2, Subtitle A, Chapter II, Part 200) the following provisions apply, as applicable:

a. Rights to Inventions. If Supplier is a small business firm or nonprofit organization, and is providing experimental, development, or research work under this transaction, Supplier must comply with the requirements of 3 CFR Part 401, "Rights to Inventions Made by nonprofit Organizations and Small Business Firms Under Government Grants, Contracts, and Cooperative Agreements".

b. Clean Air Act. Supplier agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

c. Byrd Anti-Lobbying. Supplier certifies that it will not, and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352.

d. Procurement of Recovered Materials. If Supplier is a state agency or agency of a political subdivision of a state, then Supplier must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act.

e. Domestic Preferences for Procurements. As appropriate and to the extent consistent with law, Supplier should, to the greatest extent practicable under a Federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). ''Produced in the United States'' means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States. ''Manufactured products'' means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

D. In these provisions, the term "contractor" as used therein will refer to Supplier, and the terms "Government" or "Contracting Officer" as used therein will refer to UC. Where a purchase of items is for fulfillment of a specific U.S. Government prime or subcontract, additional information and/or terms and conditions may be included in an attached supplement. By submitting an invoice to UC, Supplier is representing to UC that, at the time of submission:

a. Neither Supplier nor its principals are presently debarred, suspended, or proposed for debarment by the U.S. government (see FAR 52.209-6);

b. Supplier has filed all compliance reports required by the Equal Opportunity clause (see FAR 52.222-22); and

c. Any Supplier representations to UC about U.S. Small Business Administration or state and local classifications, including but not limited to size standards, ownership, and control, are accurate and complete.

b. Byrd Anti-Lobbying. Supplier certifies that it will not, and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352.

18. Equal Opportunity Affirmative Action.

Supplier will abide by the requirements set forth in Executive Orders 11246 and 11375, if applicable. Where applicable, Supplier will comply with 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a), incorporated by reference with this statement: "This contractor and subcontractor shall abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status or disability." With respect to activities occurring in the State of California, Supplier agrees to adhere to the California Fair Employment and Housing Act, if applicable. Supplier will not maintain or provide facilities for employees at any establishment under its control that are segregated on a basis prohibited by federal law. Separate or single-user restrooms and necessary dressing or sleeping areas must be provided, however, to ensure privacy, as applicable.

19. Conflict of Interest.

Each party affirms that, to its knowledge as of the Effective Date, no UC employee who has participated in UC's decision-making concerning the applicable Order Form as identified in writing by UC prior to execution of the Order Form has an "economic interest" in the Agreement or Supplier. A UC employee's "economic interest" means:

a. An investment worth $2,000 or more in Supplier or its Affiliate;
b. A position as director, officer, partner, trustee, employee or manager of Supplier or its Affiliate;
c. Receipt during the past 12 months of $500 in income or $440 in gifts from Supplier or its Affiliate; or
d. A personal financial benefit from the Agreement in the amount of $250 or more.

20. Audit Requirements.

The Agreement, and any pertinent financial records reasonably required to verify the fees paid under this Agreement, is subject to the examination and audit of the Auditor General of the State of California or Comptroller General of the United States or designated Federal authority for a period of up to five (5) years after final payment under the Agreement, if required by applicable law or regulation and subject to confidentiality.

21. Prohibition on Unauthorized Use or Disclosure of Institutional Information.

A. Prohibition on Use and Disclosure of Institutional Information. Institutional Information means Confidential Information. OpenAI will only use or disclose Institutional Information in accordance with Section 6 above. In addition to the terms in Section 6 above, Supplier shall have the limited right to disclose Institutional Information to Supplier's employees, contractors, and agents (including its subprocessors which Supplier uses to provide the Services) provided that: (i) Supplier shall disclose only such Institutional Information as is necessary for the

Supplier to perform its obligations and exercise its rights under this Agreement (including for safety features within the Services), and (ii) Supplier informs such employees, contractors and agents (including its subprocessors which Supplier uses to provide the Services) of the obligations governing the access, use and disclosure of Institutional Information prior to Supplier's disclosure. Supplier shall be liable for any breach of this Agreement by such employees, contractors and agents. For avoidance of doubt, this provision prohibits Supplier from using for its own benefit Institutional Information except as contemplated herein. For the avoidance of doubt, the sale of Institutional Information is expressly prohibited.

B. Compliance with Applicable Laws and Industry Standard Practices. Supplier agrees to comply with all applicable data protection state, federal, and foreign laws, as well as industry standard practices, governing the collection, access, use, disclosure, safeguarding and destruction of Institutional Information. Supplier agrees to protect the privacy and security of Institutional Information according to all applicable data protection laws and industry standard practices, and no less rigorously than it protects its own information but in no case less than reasonable care.

C. For the avoidance of doubt, as applicable to Supplier's Services, Institutional Information may include any information that identifies or is capable of identifying a specific individual, including but not limited to:

a. Personally identifiable information,

b. Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA regulations (including, but not limited to 45 C.F.R. § 160.103),

c. Medical information as defined by California Civil Code § 56.05,

d. Cardholder data,

e. Student records, or

f. Individual financial information that is subject to laws restricting the use and disclosure of such information, including but not limited to:

i. Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 et seq.);

ii. The federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2));

iii. The federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g);

iv. The federal Fair and Accurate Credit Transactions Act (15 U.S.C. § 1601 et seq.);

v. The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq), and

vi. Applicable international privacy laws, including, but not limited to the General Data Protection Regulation.

D. Required Disclosures of Confidential Information. If either party is required by a court of competent jurisdiction, applicable law or regulation, or an administrative body to disclose Confidential Information (including the Agreement itself or any of its terms and conditions), such party will notify the other party in writing without undue delay upon receiving notice of such requirement and prior to any such disclosure (unless such party is prohibited by law from doing so), to give the other party an opportunity to oppose or otherwise respond to such disclosure. To the extent such party is still required to disclose Confidential Information, such party will furnish only that portion that is legally required and will exercise all reasonable efforts to obtain reliable assurance that confidential treatment will be afforded to any Confidential Information.

E. No Offshoring. Supplier's processing and storage of Institutional Information for ChatGPT Enterprise outside the United States, is prohibited except with prior written authorization by UC.

F. Conflict in Terms. UC's Appendix – Data Security, Appendix – BAA, and/or Appendix GDPR will control in the event that one or more appendices is incorporated into the Agreement and conflicts with the provisions of this Article.

G. Acknowledgement. Supplier acknowledges that remedies at law would be inadequate to protect UC against any actual or threatened breach of this Section by Supplier, and, without prejudice to any other rights and remedies otherwise available to UC, and UC may seek injunctive relief.

22. UC Whistleblower Policy.

22.1 UC is committed to conducting its affairs in compliance with the law, and has established a process for reporting and investigating suspected improper governmental activities. Please visit http://www.ucop.edu/uc-whistleblower/ for more information.

23. Sustainable Procurement Guidelines.

Supplier will conduct business using environmentally, socially, and economically sustainable products and services to the maximum possible extent consistent with the Agreement by complying with the obligations set forth at: www.openai.com/policies/supplier-code.

Supplier will adhere to all applicable environmental laws, regulations, permits, and standards (the "Sustainability Standards"). Supplier acknowledges that failure to comply with any of the Sustainability Standards in the Agreement will constitute a material breach of the Agreement and UC will have the right to terminate the Agreement in accordance with Section 10 without damage, penalty, cost or further obligation.

Electronic Transfer of Supplier Information. Each party will use commercially reasonable efforts to (i) refrain from providing hard copies of presentations, marketing material, or other informational materials and (ii) present all information in electronic format that is easily transferable to applicable staff. Materials may be provided in hard copy or physical format if specifically required or requested by a representative.

24. Miscellaneous.

24.1 *Headings*. Headings in this Agreement are inserted solely for convenience and are not intended to affect the meaning or interpretation of this Agreement.

24.2 *Feedback*. If Customer provides OpenAI with feedback regarding the Services ("**Feedback**"), Customer grants OpenAI the right to use and exploit Feedback without restriction or compensation.

24.3 *Publicity*. During the Term, OpenAI may (a) subject to Customer's separate written consent, use Customer's name, logo and marks ("Marks") to identify Customer as a customer of the Services in marketing materials and on OpenAI's website, and (b) subject to Customer's mutual agreement in each case, produce and publish a case study regarding Customer's use of the Services. OpenAI will use Marks provided by Customer in accordance with any brand guidelines that Customer provides to OpenAI prior to such use. Customer may use OpenAI's Marks to describe its use of the Services solely in accordance with OpenAI's Brand Guidelines available at: https://openai.com/brand.

24.4 *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.

24.5 *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. Customer agrees that any terms and conditions contained within any purchase order Customer sends to OpenAI will not apply to this Agreement and are null and void. In the event of any conflict between the documents that make up this Agreement, unless explicitly stated otherwise, the order of precedence will be (a) the OpenAI Policies, (b) the applicable Order Form, and (c) this Agreement.

24.6 *Relationship of the Parties*. For all purposes under this Agreement, Customer and OpenAI will be and act as independent contractors and will not bind nor attempt to bind the other to any contract.

24.7 *No Third Party Beneficiaries*. Nothing in the Agreement, express or implied, is intended to make any person or entity that is not a signer to the Agreement a third-party beneficiary of any right created by this Agreement or by operation of law.

24.8 *Force Majeure*. Except for payment obligations, neither Party shall be deemed to be in default of or to have breached any provision of this Agreement due to a delay, failure in performance or interruption of service, if such

performance or service are impossible to execute, illegal or commercially impracticable, because of the following "force majeure" occurrences: acts of God, acts of civil or military authorities, civil disturbances, wars, strikes or other labor disputes, transportation contingencies, freight embargoes, acts or orders of any government or agency or official thereof, earthquakes, fires, floods, unusually severe weather, epidemics, pandemics, quarantine restrictions and other catastrophes or any other similar occurrences beyond such party's reasonable control. In every case, the delay or failure in performance or interruption of service must be without the fault or negligence of the Party claiming excusable delay and the Party claiming excusable delay must promptly notify the other Party of such delay. Performance time under this Agreement shall be considered extended for a period of time equivalent to the time lost because of the force majeure occurrence; provided, however, that if any such delay continues for a period of more than thirty (30) days, either Party shall have the option of terminating this Agreement upon written notice to the other Party.

24.9 *Assignment*. This Agreement cannot be assigned other than as permitted under this Section 25.9 (Assignment). Except as to any payment due hereunder, Supplier may not assign the Agreement without UC's written consent except to an Affiliate or to a successor to substantially all the respective party's assets or business, provided that the assigning party provides reasonable (at least 30 days) prior written notice of the assignment. The assignee will be subject to all of the terms of the Agreement.

24.10 *Notices*. All notices will be in writing. OpenAI may provide Customer notice using the registration information or the email address associated with Customer's account. Service will be deemed given on the date of receipt if delivered by email or on the date sent via courier if delivered by post. OpenAI accepts service of process at this address: OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, Attn: contract-notices@openai.com.

24.11 *Waiver*. Waiver or non-enforcement by either Party of a provision of the Agreement will not constitute a waiver or non-enforcement of any other provision or of any subsequent breach of the same or similar provision.

24.12 *Severability*. If a provision of the Agreement becomes, or is determined to be, illegal, invalid, or unenforceable, that will not affect the legality, validity or enforceability of any other provision of the Agreement or of any portion of the invalidated provision that remains legal, valid, or enforceable.

24.13 *Amendments*. The Parties may make changes in the Goods and/or Services or otherwise amend the Agreement, but only by a writing signed by both Parties' authorized representatives. In the event there is a Material Change to the Agreement, the parties agree to meet and confer in good faith in order to modify the terms of the Agreement. A Material Change as used herein refers to:

a. A change to the scope of Goods and/or Services to be provided by Supplier, as agreed to by UC;
b. Changes in the status of the parties;
c. Changes in flow down terms from external parties; and
d. Changes in law or regulation applicable to this Agreement.

24.14 *Other Applicable Laws*. Any provision required to be included in a contract of this type by any applicable and valid federal, state or local law, ordinance, rule or regulations will be deemed to be incorporated herein.

24.15 *Jurisdiction, Venue, and Choice of Law*. California law will control the Agreement and any document to which it is appended. 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.

24.16 *Supplier Terms*. Any additional terms that a Party includes in an order form or similar document will be of no force and effect, unless the other Party expressly agrees in writing to such terms.

24.17 *Survival Clause*. Upon expiration or termination of the Agreement, the following provisions will survive: INTELLECTUAL PROPERTY, COPYRIGHT, PATENTS, AND DATA RIGHTS; INDEMNITY AND LIABILITY; AUDIT REQUIREMENTS (to the extent set forth therein; PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF INSTITUTIONAL INFORMATION; GOVERNING LAW AND VENUE, and, to the extent incorporated into the Agreement and OpenAI continues to process personal data after expiration or termination of the Agreement, the terms of the APPENDIX–DATA SECURITY, APPENDIX–BAA, and/or APPENDIX-GDPR.

25. Incorporated Documents

This Agreement and its Incorporated Documents contain the entire agreement between the Parties, in order of the below precedent (except as set forth in Section 21 F), concerning its subject matter and shall supersede all prior or other agreements, oral and written declarations of intent and other legal arrangements (whether binding or non-binding) made by the Parties in respect thereof.

i)Enterprise Agreement
ii) Business Associate Agreement (HIPAA)
iii)Data Processing Addendum
iv)UC Appendix Data Security
v)Pricing Schedule or Order Form (as applicable) except as set forth below

26. **Purchase Order/ Order Form**

a. The terms of this Agreement will cover purchase and use of the Services by any UC Location.

b. The specific details of the Services to be purchased by each individual UC Location will be set forth in Supplier's Order Form.

c. Additional terms may also be set forth in the Order Forms. In the event of a conflict or inconsistency between the Agreement and an Order Form, the terms of the Agreement will take precedence except to the extent expressly set forth in such Order Form.

d. Supplier shall not begin providing Services until UC approves a PO against Supplier's Order Form for the Services.

e. Supplier will submit invoices following the designated invoice method directly to UC Accounts Payable Departments at each UC Location.

27. Pricing. Unless otherwise agreed to by the parties in writing, the pricing terms set forth on Exhibit B will apply to UC Order Forms under this Agreement.

Accepted and Agreed:

OpenAI, L.L.C.		**The Regents of the University of California**
Signature: Aliisa Rosenthal		Signature: Paul Williams
Name: Aliisa Rosenthal		Name: Paul Williams
Title: Authorized Signer		Title: AVP and Chief Procurement Officer
Date: 6/13/2024		Date: 6/13/2024

EXHIBIT A
ACCESSIBILITY COMMITMENTS

Open AI will use commercially reasonable efforts such that within twelve (12) months of Agreement Effective date, OpenAI will conform to the accessibility requirements of WCAG 2.1AA:

1. Engage a third party to conduct an assessment of ChatGPT conformance to accessibility standards (WCAG 2.1 AA)
2. Share with Customer the results of the assessment as soon as available, but not later than ninety 90 days following the effective date of the Agreement.
3. Share with Customer Open AI's Accessibility Conformance Report (ACR) informed by the assessment as soon as possible.
4. Establish a roadmap to meet WCAG 2.1 Level AA with dates and milestones for addressing results of the assessment and share the roadmap with Customer as soon as available, but not later than six (6) months following the effective date of the Agreement.
5. Arrange and participate in quarterly check-in meetings with Customer to present progress toward conformance. Such meetings will include OpenAI's compliance/accessibility staff.
6. Share with Customer Open AI's process and/or mechanism for addressing and testing for accessibility and advancing toward conformance.
7. Provide to Customer a plan and timeline for remediating accessibility issues that Customer identifies (for example, if Customer's users encounter a barrier to using the Services due to an accessibility issue).
8. Use commercially reasonable efforts to share product roadmap details with Customer for the purpose of reviewing accessibility and providing feedback to OpenAI.
9. Ensure all elements of the main chat interface and settings screens have accessible names / labels not later than one hundred twenty (120) days following the effective date of the Agreement.
10. Ensure the primary chat interface functionally keyboard-only & screen reader are accessible not later than six (6) months following the effective date of the Agreement.
11. Ensure any new interfaces or major features released after one hundred twenty (120) days following the effective date of the Agreement meet WCAG 2.1 Level AA or have a clear roadmap for coming into compliance stated at the time of launch.
12. Ensure ChatGPT Enterprise is WCAG 2.1 AA compliant not later than twelve (12) months following the effective date of the Agreement.
13. If ChatGPT is not WCAG 2.1 AA compliant within twelve (12) months following the effective date of the Agreement, UC may exercise its discretion to renegotiate the roadmap or terminate Agreement; provided, however, that any Order Forms in effect will continue until the end of the subscription term for such Order Form.

EXHIBIT B

PRICING TERMS

a. During the term of the Agreement, the Services shall be available for UC purchase, at UC's discretion (e.g. UC is not required to enter into Order Forms), based on the pricing/discounts set forth in the applicable Order Form. The pricing is UC net price for ChatGPT purchased under an Order Form and shall not increase during the subscription term. There shall be no additional separate charges, fees, handling or other incidental costs for ChatGPT purchased under the applicable Order Forms.

b. If Supplier makes any changes resulting in price decreases to its standard list price for ChatGPT, such decreased pricing will be made available to UC and the parties will work in good faith to amend the applicable Order Form.

c. For successive renewal periods of ChatGPT under an applicable Order Form, Supplier's subscription fees for the existing Services under such Order Form shall not exceed 3% percent per renewal period. Supplier agrees that for each renewal term, the increase shall be a one-time increase as reflected in the renewal Order Form.

d. Because there is no mandatory use policy at UC, nothing in this Agreement shall be construed to prevent UC from entering into similar agreements with any other partners including, without limitation, suppliers that may be in competition with the Supplier.

e. Once UC meets the minimum End User purchase threshold inclusive of all UC Locations (the "Minimum Threshold"), pricing for ChatGPT will not exceed the following:

ChatGPT EDU

Minimum Threshold: 10,000 End Users

10,000-19,999 End Users - $12/user/month
20,000 - 35,000 End Users - $11/user/month
35,000+ End Users - $10/user/month

ChatGPT Enterprise

Minimum Threshold: 1,000-9,999: $30/user/month

Electronic Record of Contracts

This document was generated as a record of certain contracts created, accepted and stored electronically.

Summary of Contracts

This document contains the following contracts.

Title	ID
Enterprise Agreement (The Regents of the University of California and OpenAI)	abca8b9a-922f-492f-b5ad-6e88e1728fff

Contracts signed by:

Paul Williams

Signer ID: e41398e8-e888-4b90-b364-3b7f15a33743
Email: paul.williams@ucop.edu

Date / Time: Jun 13, 2024 at 6:34 AM EDT
IP Address: 67.188.54.29
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36

Aliisa Rosenthal

Signer ID: 5b30ffe2-1732-4275-a1d7-2072b83c3a68
Email: aliisa@openai.com

Date / Time: Jun 13, 2024 at 11:07 AM EDT
IP Address: 73.223.37.66
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

UNIVERSITY OF CALIFORNIA

UC APPENDIX DATA SECURITY (as modified and agreed by both parties)

ARTICLE 1. PURPOSE AND INTRODUCTION

A. In the course of providing the Goods and/or Services contemplated by the Agreement, Supplier may gain access to the University of California's (UC) Institutional Information and/or IT Resources (both defined below). In such an event, UC and Supplier desire to appropriately protect Institutional Information and IT Resources. The purpose of this Appendix-Data Security is to specify Supplier's cybersecurity and risk management responsibilities when Supplier has access to Institutional Information and/or IT Resources.

B. Any capitalized terms used here have the meaning ascribed to such terms as set forth in the Agreement or Incorporated Documents.

C. Supplier must provide commercially reasonable cybersecurity and cyber risk management designed to protect Institutional Information and/or IT Resources. This must include, but is not limited to the Supplier:

1. Developing and documenting a plan that protects Institutional Information and IT Resources.
    - Supplier must responsibly execute this plan.
    - Supplier's approach must conform to a recognized cybersecurity framework designed for that purpose.[1]
    - Supplier's information security plan must be supported by a third-party review or certification. Supplier may only use an alternative to a third-party review if approved by the responsible UC Information Security Officer.

2. Conducting an accurate and thorough assessment of the potential risks to and vulnerabilities of the security of the Institutional Information and/or IT Resources as set forth herein. Supplier must mitigate anticipated risks effectively. This includes implementing commercially acceptable security policies, procedures, and practices that protect Institutional Information and/or IT Resources.

3. Updating its plan to effectively address new cybersecurity risks.

4. Complying with pertinent contractual and regulatory responsibilities.

5. Providing UC with reasonable evidence of compliance with Supplier's information security plan to demonstrate compliance with this Appendix and applicable data protection laws at UC's request and no more than once per year except as explicitly set forth herein.

6. Using commercially reasonable efforts to keep UC informed with timely updates on risks, vulnerabilities, Security Incidents, and Breaches.

7. Using commercially reasonable efforts to keep UC informed of any

measures UC must perform to ensure the security of Institutional Information and IT Resources in connection with UC's use of the Goods and/or Services.

[1] Examples include the latest versions of PCI DSS, NIST CSF, CIS Critical Security Controls, IS0 27000 series, NIST SP 800-53 and NIST SP 800-171, and SSAE 16/ISAE 3402 Type 2.

D. If, in the course of and in connection with providing the Goods and/or Services under the Agreement, Supplier engages in transactions with UC affiliated individuals (including but not limited to: students, staff, faculty, customers, patients, guests, volunteers, visitors, research subjects, etc.), under the Agreement, Supplier must treat any data about UC affiliated individuals that Supplier creates, receives, and/or collects in the course of those transactions with the same level of privacy and security protections and standards as required of Institutional Information by this Appendix.

E. Supplier agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Supplier also agrees to impose, by written contract, substantially the same terms and conditions contained in this Appendix on any sub-supplier retained by Supplier to provide or assist in providing the Goods and/or Services to UC.

F. To the extent that a requirement of this Appendix conflicts with the Agreement or Incorporated Document, the most stringent requirement (including but not limited to: least risk to UC, shortest time, best practice, etc.) will apply.

ARTICLE 2. DEFINED TERMS

A. "Breach" means: (1) Any disclosure of Institutional Information to an unauthorized party or in an unlawful manner; (2) Unauthorized or unlawful acquisition of information that compromises the security, confidentiality, or integrity of Institutional Information; or (3) The acquisition, access, use, or disclosure of UC protected health information (PHI) or medical information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) or California law.

B. "Illicit Code" means: (1) Hidden software or functionality with materially adverse or undesired actions or consequences to IT Resources or Institutional Information; (3) Code that replicates or transmits Institutional Information or activates operating systems or other similar services without the knowledge and approval of UC except as provided under the Agreement; (4) Code that alters, damages, or erases any Institutional Information or software without the knowledge and approval of UC except as provided under the Agreement; or (5) Code or apparatus that functions in any way as a: key lock, node lock, time-out, "back door," "trap door," "booby trap," "dead drop device," "data scrambling device," or other function, regardless of how it is implemented, which is intended to alter or restrict the use of or access to any Institutional Information and/or IT Resources.

C. "Institutional Information" is defined in the Enterprise Agreement, Section 22A.

D. “IT Resource” means: IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability that is UC owned/managed that Supplier has access to in connection with its supply of Goods and/or Services. IT Resources include, but are not limited to: personal and mobile computing systems and devices,

mobile phones, printers, network devices, industrial control systems (including but not limited to: SCADA, PLCs, DPC, Operational Technology, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens, or Internet of Things (IoT).

E. "Major Change" means: The implementation of a change in Supplier's security measures that could have a significant adverse effect on the security of an IT Resource or Institutional Information. The scope includes changes to architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items. These include changes related to:

1. Technology upgrades or migrations.
2. Responses to Security Incidents.
3. Modifications of scope (data elements, features, location of Institutional Information, etc.).
4. Regulatory guidance.
5. Law and legal regulations.
6. Responses to risk assessments.
7. Addressing vulnerabilities.
8. Material updates or shifts in technologies used by Supplier.

F. "Personal Information" has the meaning assigned to the term "personal data" or "personal information" under applicable data protection laws.

G. "Security Incident" means any of the following as it relates to Supplier's processing of Institutional Information under the Agreement: (1) A material compromise of the confidentiality, integrity, or availability of Institutional Information; (2) A single event or a series of unwanted or unexpected events that has a significant likelihood (after reasonable investigation) of compromising threatening Institutional Information; (3) Any event involving a cyber intrusion that leads to a Breach; or (4) A material failure of Supplier's administrative, technical, or physical controls that resulted or likely could result in an adverse impact to the confidentiality, integrity, or availability of Institutional Information.

ARTICLE 3. ACCESS TO INSTITUTIONAL INFORMATION AND IT RESOURCES

A. Supplier must limit its access to, use of, and disclosure of Institutional Information and IT Resources to the least invasive degree necessary required to provide the Goods and/or Services.

1. Supplier may not access or use Institutional Information and IT Resources for any purpose except to provide the Goods and/or Services.
2. For the avoidance of doubt, Supplier may not access, use, or disclose Institutional Information and IT Resources outside the scope of the Agreement for purposes of, including but not limited to: marketing, advertising, research, sale, or licensing unless expressly approved in writing by UC.

B. In the event that Goods and/or Services include the review of a specific Security Incident or a threat to or anomaly in Institutional Information or IT Resources, Supplier

must limit inspection to the least invasive degree necessary required to perform the investigation.

ARTICLE 4. SUPPLIER'S INFORMATION SECURITY PLAN AND RESPONSIBILITIES

A. Supplier acknowledges that UC must comply with information security standards as required by law, regulation, and regulatory guidance, as well as by UC's internal security program that protects Institutional Information and IT Resources.

B. Supplier must establish, maintain, comply with, and responsibly execute its information security plan.

C. Supplier's initial information security plan is attached to the Data Processing Addendum between the parties.

D. Updates to Supplier's initial information security plan will occur as follows:

1. On an annual basis, Supplier will review its information security plan, update it as needed, and, if such updated information security plan materially reduces the protections related to Institutional Information processed by or on behalf of Supplier, submit it upon written request by UC.

2. In the event of a Major Change, Supplier will review its information security plan and update it as needed (in Supplier's sole discretion).

E. If Supplier makes any material modifications to its information security plan that will reduce the overall security of Institutional Information and IT Resources, Supplier must notify UC within seventy-two (72) calendar hours and identify the changes.

F. Supplier's Information Security Plan must be designed to:

1. Ensure the security (including but not limited to: confidentiality, integrity, and availability) of Institutional Information and IT Resources through the use and maintenance of appropriate administrative, technical, and physical controls;

2. Protect against any reasonably anticipated threats or hazards to Institutional Information and IT Resources;

3. Address the risks associated with Supplier having access to Institutional Information and IT Resources;

4. Address applicable regulations;

5. Comply with all applicable legal and regulatory requirements for data protection, security, and privacy in the provision of the Goods and/or Services hereunder;

6. Clearly document the cybersecurity responsibilities of each party;

7. Follow UC records retention requirements outlined in the Agreement;

8. Prevent the sharing of passwords or authentication secrets that provide access to Institutional Information and/or IT Resources;

9. Prevent the use of passphrases (passwords) or other authentication secrets that are common across customers or multiple unrelated UC sites or units;

10. Prevent unauthorized access to Institutional Information and IT Resources;

11. Prevent unauthorized changes to IT Resources;

12. Prevent the reduction, removal, or turning off of any security control relating to Supplier's processing of Institutional Information under the Agreement without express written approval from UC (which approval may be within the Goods and/or Services);

13. Limit Supplier and sub-supplier access to Institutional Information and/or IT Resources to only those with a need to know and pursuant to a documented approval process.

14. Prevent the storing, harvesting, or passing through of UC credentials (username, password, authentication secret, or other factor); and

15. Prevent the use or copying of Institutional Information for any purpose not authorized or contemplated under the Agreement or any associated Statement of Work (SOW).

ARTICLE 5. REQUESTS FROM UC AND EVIDENCE OF COMPLIANCE

A. Supplier must provide UC with evidence that demonstrates to UC's reasonable satisfaction Supplier's adherence to its information security plan (including but not limited to: third-party report, attestation signed by an authorized individual, attestation of compliance by a qualified assessor, or a mutually agreed upon equivalent) upon execution of the Agreement and UC's request, upon reasonable request limited to annually, and/or as a result of a Security Incident, or as required by any applicable regulatory or governmental authority.

B. Supplier must respond to UC's reasonable questions related to Security Incidents, or Major Changes, newly published vulnerabilities, and/or risk assessments within a commercially reasonable period of time in accordance with Supplier's policies or as otherwise set forth herein.

C. UC may request and perform a security audit using a qualified third party or a mutually agreed upon alternative annually where required by applicable law or as a result of a Breach in order to confirm that Supplier is processing Institutional Information in a manner consistent with this Appendix; provided that any such audit is (i) subject to reasonable notice and appropriate confidentiality agreements, (ii) done in a manner that is minimally disruptive to Supplier's business, and (iii) at UC's sole expense. **Where a third-party audit or certification report addresses UC's requested scope of audit,** Supplier may instead make available to UC a summary of the results of a qualified third-party audit or certification reports relevant to Supplier's compliance with this Appendix that have been completed within twelve (12) months of the date of UC's audit request and for which Supplier confirms there are no known material changes in the controls audited. Such results, and/or the results of any assessments, audits, or other steps shall be confidential information of Supplier.

ARTICLE 6. NOTIFICATION OF MAJOR CHANGES AND VULNERABILITY DISCLOSURES

A. Supplier must notify UC without undue delay regarding changes in Supplier's security posture or IT infrastructure as follows:

1. When Major Changes happen.
2. When Supplier becomes aware of a vulnerability that warrants a CVE rating of "High" or "Critical," based on the latest CVE version, for which a

patch is not yet available or for which Supplier will delay application of an available patch, in accordance with Supplier policies.

B. Supplier must use commercially reasonable efforts to remediate any vulnerability rated as CVE High or Critical.

C. In response to Major Changes, Supplier will update its information security plan as it deems necessary within a commercially reasonable timeframe and provide updated evidence of compliance with the information security plan subject to Section 5A.

[2] Common Vulnerabilities and Exposures (CVE) is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures maintained by The MITRE Corporation. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools. The CVE list can be found at: cve.mitre.org

ARTICLE 7. RETURN AND DISPOSAL OF INSTITUTIONAL INFORMATION

A. Upon the termination, cancellation, expiration, or other conclusion of the Agreement, Supplier will return all Institutional Information to UC and dispose of the Institutional Information in possession of Supplier as detailed in the OpenAI Data Processing Addendum. This provision also applies to all Institutional Information that is in the possession of sub-suppliers or agents of Supplier.

B. Such disposal will be accomplished using industry standard methods.

C. Supplier will certify in writing (which may be email) to UC that such return and/or disposal has been completed in accordance with this Article 7, upon UC's request.

D. If Supplier believes that return and/or disposal of Institutional Information is technically impossible or impractical, Supplier must provide UC with a written statement (which may be email) explaining the reason for this conclusion. If UC determines that return and/or disposal is technically impossible or impractical, Supplier will continue to protect the Institutional Information in accordance with the terms of this Appendix for as long as the Institutional Information is in Supplier's possession.

ARTICLE 8. NOTIFICATION OF CORRESPONDENCE CONCERNING INSTITUTIONAL INFORMATION

A. Supplier agrees to notify UC promptly, but in no event more than seventy-two (72) calendar hours after Supplier receives correspondence or a complaint concerning Institutional Information that Supplier or sub-supplier processes in connection with this Agreement or is otherwise in Supplier's custody, possession or control that includes any: (i) communication that originates from law enforcement regulatory or governmental agencies unless Supplier is forbidden by binding, applicable law to inform UC, for example to preserve the confidentiality of an investigation by law enforcement authorities pursuant to a binding court order, or (ii) complaint or request directly from any individual UC data subject, but excludes normal customer service correspondence

or inquiries.

ARTICLE 9. COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS

A. Reporting of Breach or Security Incident: If Supplier reasonably suspects that a Breach and/or Security Incident impacting Institutional Information is likely (after reasonable investigation) or confirms a Breach and/or a Security Incident impacting Institutional Information, Supplier must promptly notify UC in writing using the contacts in the Agreement. Supplier must provide such notifications no later than (1) seventy-two (72) calendar hours after the initial suspicion that a Security Incident and/or Breach is likely (after reasonable investigation) and (2) seventy-two (72) calendar hours after the initial confirmation of a Security Incident and/or Breach, if Supplier is able to make such a confirmation. Supplier's notification must identify:

1. Contacts for both technical and management coordination;
2. Escalation and identifying information to the extent reasonably available, such as ticket numbers, system identifiers, etc.;
3. The nature of the Breach and/or Security Incident;
4. The Institutional Information affected;
5. What Supplier has done or will do to mitigate any deleterious effect; and
6. What corrective action Supplier has taken or will take to prevent future Security Incidents.

B. Supplier will provide other information as reasonably requested by UC.

C. In the event of a suspected Breach and/or Security Incident, Supplier will keep UC informed regularly of the progress of its investigation until the incident is resolved.

D. Coordination of Breach Response or Security Incident Activities: Supplier will reasonably cooperate with UC's investigation of any Breach and/or Security Incident involving Supplier and/or Goods and/or Services. Supplier's reasonable cooperation will include, but not be limited to, Supplier:

1. Promptly preserving any potential forensic evidence relating to the Breach and/or Security Incident as Supplier deems necessary;
2. Remedying the Breach and/or Security Incident as quickly as circumstances permit;
3. Promptly, but no more than seventy-two (72) calendar hours after the discovery of Breach and/or Security Incident, designating a contact person to whom UC will direct inquiries and who will communicate Supplier responses to UC inquiries;
4. As rapidly as circumstances permit, assigning/using commercially reasonable resources to remedy, investigate, and document the Breach and/or Security Incident and undertake commercially reasonable response activities;
5. Providing status reports to UC regarding Breach and Security Incident response activities, on a reasonable frequency;
6. Coordinating all media, law enforcement, or other Breach and/or Security

Incident notifications that identify UC or an affected UC data subject with UC in advance of such notification(s), unless expressly prohibited by law;

7. Ensuring that knowledgeable Supplier employees are reasonably available (during Supplier's normal business hours), if needed, to participate in UC and Supplier initiated meetings and/or conference calls regarding the Breach and/or Security Incident; and

8. Ensuring that knowledgeable Supplier employees and agents reasonably participate in after-action analysis, including root cause analysis and preventive action planning.

E. Steps Supplier will take to address the failures in the underlying administrative, technical, and/or physical controls to mitigate damages and future cyber risk.

F. Grounds for Termination: Any material breach of this Agreement may be grounds for termination of the Agreement by UC. Agreement obligations to secure, dispose, and report continue through the resolution of the Breach and/or Security Incident.

ARTICLE 10. ILLICIT CODE WARRANTY[3]

A. Supplier represents and warrants that it will employ industry standard measures designed to ensure that the Goods and/or Services do not contain Illicit Code.

B. Should Supplier learn of the presence of Illicit Code, Supplier will promptly provide UC with written notice (which may be email) explaining the scope and associated risk to Institutional Information or IT Resources (if any).

C. Supplier represents and warrants that it will take commercially reasonable steps to promptly remove Illicit Code adversely affecting the provision of the Goods and/or Services hereunder.

ARTICLE 11. BACKGROUND CHECKS

A. Before Supplier's employee, sub-supplier, or agent may access Institutional Information and/or IT Resources classified at Protection Level 3 or Protection Level 4[4], Supplier must conduct an industry standard background check (where legally permissible) or commercially reasonable due diligence (if a sub-supplier). Supplier must evaluate the results prior to granting access in order to reasonably assure that there is no indication that the employee, sub-supplier, or agent presents a risk to Institutional Information and IT Resources.

B. Supplier must retain each employee's, sub-supplier's, or agent's background check documentation for a period of three (3) years following the termination of the Agreement.

[3] This provision does not relate to malware or viruses that attack the running IT Resource. These are covered under ARTICLE 9 - COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS.
[4] See Exhibit 1.

Aliisa Rosenthal

Aliisa Rosenthal

Member of Go To Market Staff

6/12/2024

Paul Williams

Paul Williams

AVP and Chief Procurement Officer

6/12/2024

OpenAI Data Processing Addendum

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 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.

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 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. If Appendix DS applies to this Agreement, "Customer Data" as used herein shall also be considered UC Institutional Information as defined in Appendix DS.

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 a "**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, but only to the extent such Subprocessor processes Customer Data in the United States. A Subprocessor may only process Customer Data outside the United States with the prior express written consent of Customer. 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 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. OpenAI shall 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 upon the following occurrences: (1) reasonable request no more than once per year; (2) immediately upon any material changes to OpenAI's privacy or security policies that materially diminish the protections provided to UC herein; or (3) immediately upon any changes to OpenAI's privacy or security policies that materially alter the processing of Customer Data, including but not limited to, changes relating to purposes of processing, the categories of recipients of Customer Data, the retention period of Customer Data, the transfer of Customer Data outside the United States, or the lawful basis for proceeding;

i. 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 (unless such assessments, audits, or other steps reveal a breach by OpenAI of this DPA or such assessments, audits, or other steps are performed by or on behalf of Customer are in response to a breach by OpenAI of this DPA, in which case OpenAI will bear the reasonable direct costs) 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. Such assessments, audits, or other steps performed by or on behalf of Customer shall occur no more than once per year, unless to the extent the assessment, audit,

or other steps performed are in response to a likely (after reasonable investigation) confirmed breach by OpenAI of this DPA. Where permitted by law and only to the extent a third-party audit or certification report addresses Customer's requested scope of an assessment, audit, or steps performed, 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 deidentified, anonymized, and/or aggregated form (as such terms are defined or interpreted under the applicable U.S. Privacy Law) as part of the Services. OpenAI, 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 reidentify the information, except that OpenAI may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes comply with Data Protection Laws or are functioning as intended; and (iii) before sharing deidentified 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 and other laws applying to such data, but only to the extent such uses are expressly permitted by the Agreement and such Customer Data is: (i) not combined in a manner such that the data can infer information about, or otherwise link to a particular person or household, or (ii) not combined in a manner such that individuals can be re-identified.

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 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, Subprocessors, Subprocessor personnel, and others to whom OpenAI provides access to Customer Data 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 Data Protection Laws applicable to Customer.
   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 that are not offered by OpenAI and that Customer, and not OpenAI, is responsible for implementing those configurations and design decisions, including those configurations and design decisions that are offered by Open AI, 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. If applicable, Customer shall not take any action that would (i) render the provision of Customer Data to OpenAI a "sale" under U.S. Privacy Laws applicable to UC or a "share" under the CCPA (or equivalent concepts under U.S. Privacy Laws applicable to UC); or (ii) render OpenAI not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws applicable to UC.

7. **Standard Contractual Clauses.**
   a. OpenAI will process Customer Data that originates in the European Economic Area in accordance with the standard contractual clauses adopted by the EU Commission on June 4, 2021 ("**EU SCCs**") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
      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.
   b. 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 but only with respect to Subprocessors processing Customer Data in the United States unless otherwise agreed by the parties in writing, 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 EU member state where the data exporter is located;
vi. In Clause 18(b), disputes will be resolved before the courts of the EU member state where the data exporter is located;
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

c. Customer Data originating from Switzerland shall be processed in accordance with the EU SCCs with the following amendments:
i. "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.
ii. "Revised FADP" means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023.
iii. The term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
iv. The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.
v. The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP

d. With respect to Customer Data originating from the United Kingdom, the parties will comply with the terms of Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses (the "**UK Addendum**"). The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Annex I of Appendix 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.

OpenAI, LLC

Signature: 

Name: Aliisa Rosenthal

Title: Authorized Signer

Date: 6/12/2024

Officers of The Regents of the University of California

Signature: 

Name: Paul Williams

Title: AVP and Chief Procurement Officer

Date: 6/12/2024

Exhibit A

ANNEX I

A. LIST OF PARTIES

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

Data importer(s):

Name: OpenAI, LLC

Address: 3180 18th St., San Francisco, CA 94110

Contact Person's name, position and contact details:

Sheila Dunning
Head of Commercial Legal
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: Sheila Dunning 8/24/2023

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 appendix is attached.

Purpose(s) of the data transfer and further processing

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

C. COMPETENT SUPERVISORY AUTHORITY

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

The data protection authority of the EU Member State in which the exporter is established.

Exhibit B

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL 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 Addendum 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 the Services (the "Customer Data"). Capitalized terms not defined in this Annex II 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 Security Portal at https://trust.openai.com/ (the "Security Portal"). The Security Measures below include the subset of the information available in the Security 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; *for clarity, the ChatGPT Enterprise Service was not included in past penetration testing and will be included in a penetration test by the end of 2023*;
- 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, *provided that for ChatGPT Enterprise, SOC 2 Type II audits will be initiated by the end of 2023, and OpenAI will share summary details when available*; 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.

Electronic Record of Contracts

This document was generated as a record of certain contracts created, accepted and stored electronically.

Summary of Contracts

This document contains the following contracts.

Title	ID
Data Processing Agreement (Officers of The Regents of the University of California and OpenAI)	81715262-16c3-41c9-a869-3db894f712da

Contracts signed by:

Paul Williams

Signer ID: 4ab376d7-98f8-4ece-b586-2f27aa4b793d
Email: paul.williams@ucop.edu

Date / Time: Jun 12, 2024 at 8:36 PM EDT
IP Address: 128.48.6.159
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36

Aliisa Rosenthal

Signer ID: 3c0f0480-85c6-4a83-b1dd-4dd7d6eb4200
Email: aliisa@openai.com

Date / Time: Jun 13, 2024 at 12:27 AM EDT
IP Address: 73.223.37.66
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

HEALTHCARE ADDENDUM

This Healthcare Addendum (together with the BAA, this "**Healthcare Addendum**") is entered into by OpenAI, L.L.C. ("**OpenAI**"), and Officers of The Regents of the University of California ("**Customer**") as of the last date set forth below, and supplements the OpenAI Business Terms or other agreement for services entered into by OpenAI and Customer (together with this Healthcare Addendum, the "**Agreement**").

1. Definitions. The following definitions shall apply for purposes of this Healthcare Addendum. Capitalized terms not defined below shall have the meanings ascribed to them under HIPAA, the BAA, or the Agreement.

1.1. "**BAA**" means the Business Associate Agreement attached as Exhibit A.

1.2. "**Eligible Services**" means (a) OpenAI's Zero Retention API, (b) ChatGPT Enterprise and (c) any other services OpenAI explicitly identifies as Eligible Services in writing from time to time. For the purposes of this Healthcare Addendum only, "**Services**" shall mean only the Eligible Services.

1.3. "**HIPAA**" means, collectively, the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 and the regulations promulgated thereunder, including , the regulations promulgated thereunder by the U.S. Department of Health and Human Services (45 C.F.R. Parts 160, 162 and 164) (the "HIPAA Regulations"), the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act").

1.4. "**HIPAA Input**" means Input containing PHI that Customer transmits to OpenAI through the Eligible Services.

1.5. "**HIPAA Output**" means Output that OpenAI returns to Customer in response to the HIPAA Input.

1.6. "**Personnel**" of Customer means Customer's employees and agents.

1.7. "**Third Party Offering**" means any products, services, or content offered through OpenAI services by a third party. Third Party Offerings include, without limitation, Plugins, Actions, Third Party GPTs, and collaboration features such as shared links and templates (unless otherwise permitted in the HIPAA Compliance and Implementation Guide).

1.8. "**Zero Retention API**" means OpenAI's solution for processing Customer Content without saving, retaining, or logging such content for human review. To access OpenAI's Zero Retention API, Customer's account must indicate that Zero Retention has been activated for the Org ID in question (each, an "**Approved Org ID**").

2. Obligations of the Parties.

2.1. Eligible Services and Implementation. Customer (including its Personnel, Upstream Customers, End Users and other data custodians) may transmit and disclose PHI only through the Eligible Services and only in accordance with the terms and conditions of this Healthcare Addendum, including Sections 2 and 3 hereof and the HIPAA Compliance and Implementation Guide set forth at as Exhibit B. Without limiting the foregoing, Customer acknowledges and agrees that the following services are **not** Eligible Services and may not be used to transmit or disclose PHI: (i) Third Party Offerings, (ii) API use that is not through an Approved Org ID, and (iii) API use that is not to an endpoint eligible for Zero Retention (as set forth at: https://platform.openai.com/docs/models/default-usage-policies-by-endpoint).

2.2. Customer Content. Customer is solely responsible for (i) the development, content, and integrity of the HIPAA Input, (ii) ensuring accurate matching (including patient matching) so that HIPAA Input is properly matched to HIPAA Output, and (iii) ensuring that HIPAA Output is returned to the appropriate Upstream Customer.

2.3. Business Associate Agreement. By executing this Healthcare Addendum, the parties agree to be bound by the BAA.

3. Healthcare Restrictions and Requirements.

3.1. Healthcare Purposes Generally. For any use of the Services or use or disclosure of HIPAA Output in connection with healthcare activities (including without limitation the practice of medicine, billing, coding, claims processing, or clinical research) ("**Healthcare Activities**") Customer will: (i) test the Services for accuracy in Customer's use cases and disclose to Upstream Customers any limitations associated with HIPAA Output; (ii) ensure that Upstream Customers understand and comply with this Healthcare Addendum and all applicable laws and regulations, including by providing appropriate training; and (iii) ensure that only duly trained and qualified individuals who maintain licenses, certifications or other authorizations required to perform such Healthcare Activities will use the Services or use or disclose the HIPAA Outputs in connection with such Healthcare Activities.

3.2. Upstream Customers. Customer will enter into a written agreement with each Upstream Customer that (i) contains terms relevant to the obligations of Customer that are substantially similar to those contained in this Agreement (including this Healthcare Addendum) and (ii) requires such Upstream Customer to comply with all laws and regulations applicable to its use of the Services and HIPAA Output.

3.3. Transparency. Customer shall not represent, to an Upstream Customer or to any other party, that the Services were performed by a human or that HIPAA Output was human-generated.

3.4. Training. Customer shall train its Personnel on its obligations and responsibilities relating to this Healthcare Addendum and inform Upstream Customers and End Users, to the extent they are not Personnel, of such obligations and responsibilities relating to this Healthcare Addendum.

4. Disclaimers. Notwithstanding any warranties or other terms in the Agreement, and without limiting any disclaimers set forth in the Agreement, the Services and HIPAA Output are not intended to substitute for the function or services of properly trained and licensed individuals, including without limitation physicians or other clinicians, billing, coding, or claims personnel, or clinical researchers. OpenAI is not responsible or liable for any advice, course of treatment, diagnosis, or any other information or services that any patient or other individual may obtain or receive; billing, coding, or claims activities conducted by Customer or its Upstream Customers; or for the accuracy, completeness, or suitability of any data or information used in any Healthcare Activities, including clinical research activities conducted by Customer or its Upstream Customers. The Services and HIPAA Output are not intended to be used in a manner that constitutes a medical device.

5. Each party's liability towards the other party under or in connection with this Healthcare Addendum will be limited in accordance with the provisions of the Enterprise Agreement.

6. Term and Termination. This Healthcare Addendum shall remain in full force and effect for as long as the Agreement remains in effect, unless otherwise terminated. The termination provisions set forth in the Agreement shall apply equally to this Healthcare Addendum. If this Healthcare Addendum expires or is terminated for any reason, Customer shall not, and shall ensure that its Upstream Customers do not, transmit or otherwise disclose PHI to OpenAI by any means or methods. Upon termination or expiration of this Healthcare Addendum, any provision of this Healthcare Addendum that (a) expressly states that it survives beyond the Term or (b) should survive following the Term to fulfill its essential purpose, will survive.

7. General. A reference in this Healthcare Addendum to a regulatory section means the section as in effect or as amended. In addition, any notification required in this Healthcare Addendum to be made to OpenAI (or that is otherwise provided to OpenAI in connection with this Healthcare Addendum) shall also be sent to hipaa@openai.com. The recitals and exhibits to this Healthcare Addendum are hereby incorporated by reference into this Healthcare Addendum and made a binding part of this Healthcare Addendum. The Agreement shall remain in full force and effect and, except as modified by this Healthcare Addendum, applies equally to this Healthcare Addendum, which is hereby incorporated by reference into the Agreement and made a binding part of the Agreement. In the event of a conflict between this Healthcare Addendum and the Agreement, this Healthcare Addendum shall prevail with respect to the subject matter of this Healthcare Addendum.

Accepted and Agreed:

Officers of The Regents of the University of California: **OpenAI, L.L.C.:**

Signature: 

Name: Paul Williams

Title: AVP and Chief Procurement Officer

Date: 6/13/2024

Signature: 

Name: Aliisa Rosenthal

Title:

Date: 6/13/2024

EXHIBIT A

BUSINESS ASSOCIATE AGREEMENT

1. Purpose. OpenAI and Customer entered into an Agreement, pursuant to which OpenAI provides Customer access to certain OpenAI products and services that implicate HIPAA. For purposes of this Healthcare Addendum including this Business Associate Agreement (BAA), Customer is either a Covered Entity, or a Business Associate of its Upstream Customers. OpenAI is either a Subcontractor of Customer, or a Business Associate of Customer.

2. Definitions. The following definitions shall apply for purposes of this Business Associate Agreement.

2.1. "**Business Associate**" has the same meaning as the term "Business Associate" in 45 C.F.R. § 160.103.

2.2. "**Covered Entity**" has the same meaning as the term "covered entity" in 45 C.F.R. § 160.103.

2.3. "**HIPAA Breach Notification Rule**" means the Breach Notification for Unsecured Protected Health Information regulations, codified at 45 C.F.R. parts 160 and 164, as amended.

2.4. "**HIPAA Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. parts 160 and 164, as amended.

2.5. "**HIPAA Security Rule**" means the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. parts 160 and 164, as amended.

2.6. "**Protected Health Information**" or "**PHI**" has the same meaning as under HIPAA, limited to such information that OpenAI receives from Customer.

2.7. "**Required by Law**" has the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

2.8. "**Security Incident**" has the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

2.9. "**Subcontractor**" has the same meaning as the term "subcontractor" in 45 C.F.R. § 160.103.

2.10. "**Unsecured Protected Health Information**" or "**Unsecured PHI**" have the same meaning as under the HIPAA Breach Notification Rule, limited to such information that OpenAI receives from Customer.

2.11. "**Upstream Customer**" is a customer of Customer that is either a Covered Entity or Business Associate.

3. OpenAI Requirements and Obligations.

3.1. Prohibited Uses and Disclosures of PHI. OpenAI shall not use or disclose PHI other than as permitted or required by this BAA or the Agreement, or as Required by Law. OpenAI may not use or disclose PHI in a manner that would violate the HIPAA Privacy Rule if done by Customer or its Upstream Customers that are Covered Entities, except as provided in this BAA.

3.2. Permissible Use and Disclosure of PHI. OpenAI is permitted to collect, receive, use, maintain, create, disclose, transmit, destroy, and otherwise process PHI (i) in connection with performing its obligations and exercising its rights under the Agreement, (ii) as permitted or required by this BAA, (iii) as Required by Law, (iv) as authorized by an Individual, and (v) as otherwise permitted by applicable law. OpenAI may use PHI for the proper management and administration of OpenAI or to carry out the legal responsibilities of OpenAI. OpenAI may disclose PHI for the proper management and administration of OpenAI but only as permitted under the Agreement or to carry out the legal responsibilities of OpenAI, provided the disclosures are Required by Law, or OpenAI obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and be used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person notifies OpenAI of any instances of which it becomes aware in which the confidentiality of the PHI has been breached.

3.3. Minimum Necessary. To the extent that OpenAI uses, discloses, or requests PHI to provide the Services, OpenAI shall use reasonable efforts to limit PHI to the minimum necessary to accomplish the intended

purpose of the use, disclosure, or request, unless an exception to the minimum necessary requirements under HIPAA applies. Notwithstanding anything to the contrary, the parties acknowledge and agree that all PHI that is transmitted to OpenAI is the minimum necessary required by OpenAI to perform its obligations and exercise its rights under the Agreement.

3.4. Incident Reporting. OpenAI will report to Customer (i) any use or disclosure of PHI by OpenAI that is not permitted under this BAA of which OpenAI becomes aware, including Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410, and (ii) any Security Incident of which OpenAI becomes aware. Any such report(s) must be made promptly after, but in no case more than five (5) calendar days after, discovery by OpenAI of such impermissible use or disclosure, such Security Incident, or such Breach of Unsecured PHI. OpenAI will provide such reasonable cooperation as is reasonably requested by Customer in responding to such event and will supplement such initial report with additional information. The notification to Customer shall include, to the extent known, each individual whose Unsecured PHI has been used or disclosed by OpenAI during such Security Incident unless legally prohibited. Upon Customer's request, OpenAI shall further provide Customer with any other reasonably available information as it becomes known that Customer is legally required to include in a notification to affected individuals provided that Customer cannot obtain such information itself through the Eligible Services. The parties agree that notice is hereby deemed given for all attempted, unsuccessful Security Incidents involving trivial and routine incidents such as port scans, attempts to log-in with an invalid password or user name, denial of service attacks that do not result in a server being taken off-line, malware, and pings, or other similar types of events that do not compromise the security or privacy of PHI.

3.5. Mitigation. OpenAI will take reasonable steps to mitigate, to the extent practicable, any harmful effects known to OpenAI from any unauthorized use or disclosure of PHI by OpenAI in violation of HIPAA or this BAA

3.6. Subcontractors of OpenAI. OpenAI shall ensure that any Subcontractors of OpenAI that create, receive, maintain, or transmit PHI agree to the same restrictions and conditions that apply to OpenAI with respect to such information, to the extent required by this Healthcare Addendum. If OpenAI learns of any pattern or activity that constitutes a material breach of a Subcontractor's obligations with respect to PHI, OpenAI will take reasonable steps to cure the breach, end the violation, or terminate the relationship with its Subcontractor.

3.7. Requests for Access. The parties acknowledge and agree that OpenAI does not maintain a Designated Record Set for or on behalf of Customer or Upstream Customers. In the event that OpenAI receives a request for access to PHI under 45 C.F.R. § 164.524, OpenAI's sole responsibility shall be to promptly forward the request to Customer. In the event that Customer or any Upstream Customer receives a request for access to PHI under 45 C.F.R. § 164.524, OpenAI shall have no obligations.

3.8. Requests for Amendment. The parties acknowledge and agree that OpenAI does not maintain a Designated Record Set for or on behalf of Customer or Upstream Customers. In the event that OpenAI receives a request for amendment of PHI under 45 C.F.R. § 164.526, OpenAI's sole responsibility shall be to promptly forward the request to Customer. In the event that Customer or any Upstream Customer receives a request for amendment of PHI under 45 C.F.R. § 164.526, OpenAI shall have no obligations.

3.9. Accounting of Disclosures. In the event that OpenAI discloses PHI in a manner that is required to be included in an accounting under 45 C.F.R. § 164.528, OpenAI shall maintain and, within ten (10) business days of a request from Customer, make available such information as Customer or Upstream Customer would be required to provide an Individual requesting an accounting of disclosures under 45 C.F.R. § 164.528.

3.10. Customer Privacy Rule Obligations. The parties acknowledge and agree that OpenAI is not intended to carry out one or more of Customer's or any of Upstream Customer's obligation(s) under the HIPAA Privacy Rule.

3.11. Availability of Books and Records. OpenAI will make its HIPAA policies and any other books and records that relate to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services (or his or her designee) for purposes of determining compliance with HIPAA.

3.12. Privacy and Security Safeguards. OpenAI shall use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule (as codified in 45 C.F.R. §§ 164.302-164.318) with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this BAA.

4. Customer Restrictions and Obligations.

4.1. Compliance with Upstream Customer Business Associate Agreements. Customer shall comply with the terms and conditions of Customer's business associate agreements (entered into pursuant to 45 C.F.R. §§ 164.502(e), 164.504(e), 164.308(b), and 164.314(a)) with its Upstream Customers that are relevant to the Services.

4.2. Upstream Customer Limitation(s) in Notice of Privacy Practices. Customer shall ensure that there are no limitation(s) in its own notice of privacy practices and that of any Upstream Customer under 45 C.F.R. § 164.520 that may affect OpenAI's use or disclosure of PHI pursuant to the Agreement.

4.3. Permissions, Authorizations, and Consents. Customer represents and warrants that any permissions, authorizations (including authorizations under 45 C.F.R. § 164.508), or consents that may be required for OpenAI to provide Services, or to otherwise collect, receive, use, maintain, create, disclose, transmit, destroy, or otherwise process PHI as permitted or required under this BAA, have been obtained and reasonably documented.

4.4. Restrictions on the Use and Disclosure of PHI. Customer shall ensure that Customer and Upstream Customers have not agreed to, or are not otherwise required to abide by, restrictions on the use or disclosure of PHI under 45 C.F.R. § 164.522 that may affect OpenAI's use or disclosure of PHI pursuant to the Agreement.

4.5. Permissible Requests by Customer. Customer shall not ask OpenAI to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by Customer or any Upstream Customer. Customer shall not request that OpenAI collect, receive, use, maintain, create, disclose, transmit, maintain, destroy, or otherwise process PHI in any manner that violates HIPAA or any other applicable law or regulation.

4.6. Mitigation. Customer shall take reasonable steps to mitigate, to the extent practicable, any harmful effects known to Customer of a breach of this BAA by Customer.

5. Term and Termination. The term of this BAA shall begin on the first date Customer transmits PHI to OpenAI pursuant to the Agreement and shall continue for as long as the underlying Agreement remains in effect unless the Healthcare Addendum is otherwise terminated in accordance with Section 6 above.

Termination for Cause. Either party may terminate this Healthcare Addendum, including the BAA if it determines that the other party has violated a material term of the BAA, in accordance with the terms of the Agreement. Upon termination of this BAA for any reason, with respect to PHI received from Customer, OpenAI shall return to Customer or destroy, all such PHI that OpenAI still maintains in any form, and retain no copies of such PHI. To the extent return or destruction of Customer PHI is not feasible, OpenAI shall (1) retain only that PHI which is necessary for OpenAI to continue its proper management and administration or to carry out its legal responsibilities; and (2) continue to use appropriate safeguards for such Customer PHI and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as OpenAI retains the PHI.

6. General. In the event of a conflict between this BAA and the Agreement, this BAA shall prevail with respect to the subject matter of this BAA.

EXHIBIT B

HIPAA COMPLIANCE AND IMPLEMENTATION GUIDE

HIPAA Compliance at OpenAI

Under the Health Insurance Portability and Accountability Act ("HIPAA"), certain information about a person's health, health care and payment for health care constitutes Protected Health Information (PHI). Customers that intend to transmit, upload, or communicate regarding PHI through the Eligible Services must sign a Business Associate Agreement (BAA) with OpenAI. The BAA covers only the Eligible Services as defined in the BAA. Any other products, services or features are not covered by the BAA and should not be used with PHI. Customers who have not signed a BAA with OpenAI must not use the Services in connection with PHI. Capitalized terms not defined below shall have the meanings ascribed to them under HIPAA, the BAA, or the Agreement.

Zero Retention API Terms

To the extent you or your users transmit, upload, or communicate about PHI through the API Services, you must use the Zero Retention API. The following terms and conditions apply to the Zero Retention API:

1. **Customer Obligations**. You must only use Zero Retention API for HIPAA Input and HIPAA Output. Any other use case must be submitted separately for review and approval. If Input or Output ceases to include HIPAA Input or HIPAA Output, then you must inform OpenAI and submit the updated use case for review and approval. You are responsible for ensuring all HIPAA Input is directed to Approved Org IDs (as defined in the Healthcare Addendum).

2. **Zero Retention Platform Abuse**. OpenAI may perform automated screening of the Customer Content for safety purposes (the "Safety Classifiers"), which shall consist solely of metadata (including classifier types, dates, counts and confidence scores) and shall not include any Customer Content (including summarizations of Customer Content), PHI, or any portion thereof. OpenAI may retain Safety Classifiers indefinitely. In the event the Safety Classifiers indicate persistent or material violations of law or OpenAI Policies, or OpenAI reasonably suspects that Customer is in violation of this provision, OpenAI may suspend or revoke approval for Zero Data Retention upon notice to Customer, suspend Customer's access to the Services, or take other action in its sole discretion. If OpenAI notifies Customer that its access to Zero Data Retention will be revoked or suspended, then as soon as possible after receiving such notice, Customer will cease, and will cause its users to cease, all transmissions, uploads, and communications about PHI through the API Services.

HIPAA Implementation Guide

This HIPAA Implementation Guide is provided for informational purposes only. It is intended to help customers regulated by the HIPAA to use the Eligible Services consistent with their compliance obligations. The information in this guide does not constitute legal advice and adhering to this guidance does not ensure compliance or alignment with your HIPAA obligations. Customers are responsible for independently evaluating their own specific use of the Eligible Services as appropriate to support their legal compliance obligations, as the recommendations in the guides are for certain minimum product configurations and are not exhaustive.

We may update or revise this guidance from time to time, including to provide guidance for new features or services as they are released.

General Configuration and Use Considerations

This section provides general guidance regarding certain features to consider as you configure and use the Eligible Services consistent with your HIPAA compliance obligations and risk analysis.

1. **Users.** You may not enable patients, plan members, or their families or employers to communicate with the Services through your Customer Application, or to provision them with End User Accounts for the Services.

2. **Support Requests.** When initiating a support request to OpenAI through any means, you and your End Users may not include any PHI in the support request or attach any screenshots or documents that include PHI.

3. **Designated Record Sets**. You and your End Users may not provide PHI that is part of a designated record set to OpenAI (as defined in HIPAA).

4. **Access Management.** You are responsible for configuring use of single sign-on ("SSO") to manage access and authorization and for implementing other access management requirements for your End Users when accessing the Services. Please see OpenAI's help article regarding SSO for more information.

5. **Mobile Device Management**. You, and not OpenAI, are responsible for securing devices that are used to access the Services in accordance with HIPAA. The Services do not control the encryption, geolocation, remote wiping or other helpful or required security features of devices under HIPAA. OpenAI may store some data (such as message edits in progress) locally on a device running the OpenAI app or browser session. If your company policy requires encryption of PHI at rest, you should encrypt all devices that run OpenAI applications or browser sessions.

6. **Monitoring.** You are responsible for implementing your own tools and processes for monitoring your End Users' use of the Services.

7. **Data Backup and Emergency Access.** You are responsible for implementing backup and recovery procedures for emergency access and archival of PHI.

8. **Multiple Covered Entity Data.** OpenAI allows HIPAA-regulated customers to use the Eligible Services to manage the PHI of multiple Covered Entities. You are responsible for ensuring you have all necessary permissions and approvals, including from all relevant HIPAA-regulated entities, to use the Eligible Services for PHI. If during the course of using the Services you no longer have permission from one or more Covered Entity's data, you are responsible for deleting all Customer Content, including conversations and uploaded files, that contain that Covered Entity's PHI.

9. **State Law Requirements**. Some state health information privacy and sensitive condition laws and other federal laws are more restrictive than HIPAA or impose additional requirements on the use and disclosure of identifiable health information. You are responsible for confirming that your use of the Services is consistent with applicable state and federal laws. By using the Services for processing or maintaining identifiable health information, you are representing that: (1) such use, and your disclosure of information to OpenAI through the Services, complies with applicable state and federal laws; and (2) you have obtained all necessary consents, authorizations and permissions required by applicable law to share information with OpenAI in connection with the Services.

Using ChatGPT Enterprise With PHI

When you subscribe to ChatGPT Enterprise, the full capabilities of the Services are available to you by default. It is your responsibility to configure use of the Services consistent with your HIPAA obligations and as set forth in the Healthcare Addendum. To the extent you or your End Users transmit, upload, or communicate about PHI through the Services, the following limitations apply and you will need to adhere to certain configurations:

1. **PHI-Prohibited Fields.** You and your End Users may not include PHI in any of the following:
    a. File names
    b. User profile data, including:
        i. Name
        ii. Email Address
    c. Workspace name and image
    d. GPT Content, including:
        i. Name
        ii. Description
        iii. Instructions
        iv. Conversation starters
        v. Uploaded files
    e. Support tickets or any other support requests

2. **Workspace Settings.** The "Settings" page enables you to manage the following functionalities of your ChatGPT Enterprise workspace:

    a. **Plugins and Actions.** If enabled, the use of Plugins and/or Actions can involve transmitting information to third parties that do not offer HIPAA-enabled services. It is recommended that you disable these functionalities through the "Plugins" and "Custom Actions" toggles under "Workspace GPTs."

    b. **Browse.** If enabled, the use of the web browsing capabilities can result in PHI being transmitted to a third-party website. It is recommended that you disable this functionality through the "Browsing with Bing" toggle under "Workspace GPTs."

    c. **Third-Party GPTs.** The use of GPTs developed by third parties can involve transmitting information to third parties that do not offer HIPAA-enabled services. If you enable this functionality, you are solely responsible for implementing internal policies with respect to review and use of each third-party GPT in accordance with your legal obligations under HIPAA. Otherwise, you can choose to disable this functionality by selecting "Don't Allow" under "Third Party GPTs."

    d. **Sharing.** The "Chats can be shared with…" toggle and the "GPTs can be shared with…" toggle under "Sharing" are tools that allow you to control how your End Users can share their chats and GPTs, respectively. You are solely responsible for evaluating and configuring these tools in accordance with your legal obligations under HIPAA. For example, you should only choose to enable sharing with workspace members if you have made the determination that all End Users of your workspace are authorized to access any PHI shared over chats or GPTs. The configurations are described below:

        i. If you set these sharing toggles to "Anyone," End Users are able to share their chats or GPTs externally, which could result in PHI being transmitted to third parties outside of the workspace.
        ii. If you set these sharing toggles to "Workspace members only," End Users are able to share their chats or GPTs internally, which could result in PHI being transmitted to any End User in your workspace.
        iii. If you set these sharing toggles to "No one," End Users are not able to share their chats or GPTs with others.

    Please see OpenAI's help article regarding settings for more information.

3. **Adding Users.** Before inviting a new End User to your enterprise workspace, confirm that the End User is a part of your organization and is authorized to access PHI. It is your responsibility to ensure that your organization members are familiar with the requirements in this Implementation Guide before provisioning access to them.

4. **Data Retention.** Unless earlier deleted by an End User or unless you have selected a shorter retention period, OpenAI will maintain your data for the duration of your agreement with OpenAI. You are responsible for removing any data that needs to be removed using self-service tools provided in the Services, such as the ability to delete conversations.

Using the API Services with PHI

When you use OpenAI's Application Programming Interface services ("API Services"), the full capabilities of the Services are available to you by default. It is your responsibility to use the API services consistent with your HIPAA obligations and as set forth in the Healthcare Addendum. To the extent you or your users transmit, upload, or communicate about PHI through the API Services, the following limitations apply and you will need to adhere to certain configurations:

1. **Zero Retention API.** You must only transmit, upload, or communicate about PHI through the Zero Retention API. You are responsible for ensuring all HIPAA Input is directed to Approved Org IDs (as defined in the Healthcare Addendum), and for ensuring that that you only use endpoints eligible for zero retention as set forth at: https://platform.openai.com/docs/models/default-usage-policies-by-endpoint.

Electronic Record of Contracts

This document was generated as a record of certain contracts created, accepted and stored electronically.

Summary of Contracts

This document contains the following contracts.

Title	ID
BAA (Officers of The Regents of the University of California and OpenAI)	45685cc5-8e9e-4c3e-a157-6854506b02be

Contracts signed by:

Paul Williams

Signer ID: 8b14efc1-7562-44ee-9ea3-2187b0125320
Email: paul.williams@ucop.edu

Date / Time: Jun 13, 2024 at 6:38 AM EDT
IP Address: 67.188.54.29
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36

Aliisa Rosenthal

Signer ID: 83da0dab-ceb7-4bb6-8e3f-f22685b9b9bf
Email: aliisa@openai.com

Date / Time: Jun 13, 2024 at 11:08 AM EDT
IP Address: 73.223.37.66
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36