

OpenAI Services Agreement

This OpenAI Services Agreement ("Agreement") is entered as of the Effective Date between the organization agreeing to these terms ("Customer") and the OpenAI Contracting Party defined below ("OpenAI"). In this Agreement, OpenAI and Customer are each referred to as a "Party" and collectively as the "Parties." Capitalized terms not defined in the Agreement have the meanings provided in the Order Form. Customer represents it is lawfully able to enter into this Agreement and, if it is entering into the Agreement for an entity, that it has legal authority to bind that entity. By accepting the Order Form, Customer agrees to this Agreement.

1. Services.

- 1.1. Services Term. OpenAI will deliver the Services to Customer for the Services Term. The Services Term will be listed on the Order Form. Unless the Parties agree otherwise in writing, increases in the Services purchased during a Services Term will have a prorated term ending concurrently with the then-current Services Term.
- 1.2. Renewal. Renewal Terms, if any, will be listed on the applicable Order Form. If Customer reduces its license count, quantity, or minimum commitment, OpenAI may adjust or remove discounts offered to Customer based on its prior purchase.
- 1.3. Authorized Purchasers.
 - a. Provisioning. To provision the Services, OpenAI requires the email address of the initial Authorized Purchaser to be included on the Order Form. Failure to include correct Authorized Purchaser information on the Order Form may result in delays.
 - b. Purchases. The Services may be configured to allow Authorized Purchasers to purchase additional licenses, quantities, or volumes of Services. Customer is responsible for understanding the Services settings that allow additional purchases. OpenAI will charge Customer for additional licenses, quantities, or volumes of Services for the remainder of the then-current Services Term based on Customer's then-current price unless otherwise set forth on the Order Form.
- 1.4. Affiliates.
 - a. Usage. OpenAI provisions the Services to specific entities using dedicated workspaces and organizational IDs. Customer Affiliates may use the Services under Customer's Account, which means Customer and its Affiliates usage will occur in the same workspace and under the same organizational ID. Customer will be responsible and liable for all acts and omissions of its Affiliates that access the Services in connection with this Agreement.
 - b. Separate Purchases. If Customer Affiliates' purchase and use of the Services is intended to be separate from Customer's, then the Affiliate must execute a separate Order Form. OpenAI will then create a separate workspace and organizational ID for that Affiliate and provision the Services accordingly. If Customer Affiliates enter into Order Forms under this Agreement they will be bound by this Agreement.
- 1.5. Usage-based Services. If Customer purchases Services based on usage, Customer acknowledges that OpenAI will charge Customer the Fees for the Services based on the usage calculated by OpenAI.

2. Provision.

- 2.1. General. The Agreement governs Customer's access to and use of the Services. Customer may access and use the Services in accordance with the Agreement.
- 2.2. Use. OpenAI grants Customer a non-exclusive right to access and use the Services during the Term. This includes the right to use OpenAI's API to integrate the Services into Customer Applications and to make Customer Applications available to End Users.
- 2.3. Modifications. OpenAI may update the Services periodically. If an OpenAI update materially reduces the Services functionality, OpenAI will notify Customer at the Account email address. Within five business days of receipt of this notice, Customer may choose to terminate the Agreement by providing thirty days written notice. This termination right will not apply to updates made to features provided on a beta or evaluation basis. In the event that OpenAI discontinues Services that Customer has contracted for, Customer shall be entitled to a pro rata refund for any fees paid not used.

3. Customer Obligations.

- 3.1. Customer Account. Customer must provide accurate and current Account information. Customer will not share Account access credentials or individual login credentials between multiple users. Customer may not resell or lease

access to its Account or any End User Account. Customer will promptly notify OpenAI if it becomes aware of unauthorized access to the Account or the Services.

- 3.2. End Users. End User Accounts may only be provisioned to, registered for, and used by, a single End User. Customer is responsible for all activities that occur under its Account, including the activities of End Users with an End User Account or who access the Services through a Customer Application. Customer will obtain and maintain from End Users any consents necessary to allow Administrators to engage in the activities described in the Agreement and to allow OpenAI to deliver the Services.
- 3.3. Restrictions. Customer will not, and will not permit End Users to: (a) use the Services or Customer Content in a way that violates applicable laws or OpenAI Policies; (b) use the Services or Customer Content in a way that violates third parties' rights; (c) allow minors to use OpenAI Services without consent from their parent or guardian; (d) Reverse Engineer any aspect of the Services or the systems used to provide the Services; (e) except for a Permitted Exception, use Output to develop artificial intelligence models that compete with OpenAI's products and services; (f) extract data from the Services other than as permitted through the Services; (g) buy, sell, or transfer API keys from, to, or with a third party; (h) interfere with or disrupt the Services, including circumvent any rate limits or restrictions or bypass any protective measures or safety mitigations for the Services; (i) violate or circumvent Usage Limits or otherwise configure the Services to avoid Usage Limits.
- 3.4. Third-Party Services. Third-Party Services may be available through the Services, which Customer may elect to use in its sole discretion. Customer's access or use of Third-Party Services are governed by this Agreement and the relevant Third-Party Service Terms.

4. Customer Content.

- 4.1. Generally. Customer and Customer's End Users may provide Input and receive Output. As between Customer and OpenAI, to the extent permitted by applicable law, Customer: (a) retains all ownership rights in Input; and (b) owns all Output. OpenAI hereby assigns to Customer all OpenAI's right, title, and interest, if any, in and to Output.
- 4.2. OpenAI Obligations. OpenAI will only use Customer Content as necessary to provide Customer with the Services, comply with applicable law, enforce the OpenAI Policies, and prevent abuse. OpenAI will not use Customer Content to develop or improve the Services, to train any models (except for fine-tuning, embeddings, and similar activities conducted solely for the benefit and use of Customer), or otherwise for commercial advantage unless Customer explicitly agrees to such use.
- 4.3. Customer Obligations. Customer is responsible for all Input and represents and warrants that it has all rights, licenses, and permissions required to provide Input to the Services. Customer is solely responsible for all use of the Outputs and for evaluating the accuracy and appropriateness of Output for Customer's use case.
- 4.4. Similarity of Output. Due to the nature of OpenAI's Services and artificial intelligence generally, Output may not be unique, and other users may receive similar content from OpenAI's services. Responses that are requested by and generated for other users are not considered Customer's Output.

5. Security and Privacy.

- 5.1. Security Measures. OpenAI will comply with the Security Measures. OpenAI may periodically update the Security Measures. If OpenAI updates the Security Measures in a manner that materially diminishes the administrative, technical, or physical security features of the Services taken as a whole, Customer may elect to terminate the Agreement and associated Order Forms by providing written notice to OpenAI within five business days of becoming aware of the update.
- 5.2. Audit Reports. OpenAI has completed audits, conducted by an independent auditor, that evaluated the design and effectiveness of OpenAI security policies, procedures, and controls for the Services. Upon Customer's written request, but no more than once per year, OpenAI will provide Customer a copy of the most recent Audit Reports, which will be deemed OpenAI Confidential Information.
- 5.3. Privacy. If Customer uses the Services to process Personal Data, OpenAI and Customer will comply with the DPA, which is incorporated by this reference and attachment into the Agreement.
- 5.4. HIPAA. Customer agrees not to use the Services to create, receive, maintain, transmit, or otherwise process Protected Health Information, unless it has signed the Healthcare Addendum. NOTWITHSTANDING THE FOREGOING, NOT ALL SERVICES OFFERED BY OPENAI ARE DESIGNED FOR PROCESSING PROTECTED HEALTH INFORMATION. IF CUSTOMER USES A SERVICE THAT IS NOT DESIGNED FOR PROCESSING PROTECTED HEALTH INFORMATION, CUSTOMER MAY NOT USE THE SERVICES TO STORE, TRANSMIT, OR PROCESS THIS INFORMATION.

6. Payment.

- 6.1. Fees. Customer will pay OpenAI or Customer's reseller the applicable Fees in the currency and pursuant to the payment terms on the Order Form. If Customer's Order Form includes a minimum commitment, the minimum commitment amount is non-cancellable except as required by law, including FAR 52.212-4(l) or 52.212.4(m), or as otherwise specifically permitted in the Agreement.
- 6.2. Payment. Customer will pay OpenAI invoices or the invoices of OpenAI's authorized reseller as applicable on the payment interval set forth in the Order Form.
- 6.3. Taxes. Any taxes or surcharges which OpenAI seeks to pass along to the Government will be governed by the terms of any applicable underlying Government contract and, in any event, must be submitted to the Government for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the applicable underlying government contract.
- 6.4. Disputes. All contract disputes shall be resolved in accordance with the Contract Disputes Act, 41 U.S.C. 7101-7109, or other Disputes procedures set forth in the applicable Government contract. Overdue undisputed amounts may be subject to a finance charge in accordance with the Prompt Payment Act (31 USC 3901 et seq) and Treasury regulations at 5 CFR 1315.
- 6.5. [Reserved]
- 6.6. Corrections. OpenAI has the right to correct pricing errors or mistakes even after issuing an invoice or receiving payment in accordance with the applicable Order Form.

7. Confidentiality.

- 7.1. Use and Nondisclosure. Recipient agrees it will: (a) only use Discloser's Confidential Information to exercise its rights and fulfill its obligations under this Agreement; (b) take reasonable measures to protect the Confidential Information; and (c) not disclose the Confidential Information to any third party except as expressly permitted in this Agreement.
- 7.2. Exceptions. The obligations in Section 7.1 do not apply to information that: (a) is or becomes generally available to the public through no fault of Recipient; (b) was in Recipient's possession or known by it prior to receipt from Discloser; (c) was rightfully disclosed to Recipient without restriction by a third party; or (d) was independently developed without use of Discloser's Confidential Information.
- 7.3. Permitted Disclosure. Recipient may disclose Confidential Information only to its Affiliates, employees, contractors, and agents who have a need to know and who are bound by confidentiality obligations at least as restrictive as those in this Agreement. Recipient will be responsible for any breach of this Section 7 by its employees, contractors, and agents. Recipient may disclose Confidential Information to the extent required by law, if Recipient uses reasonable efforts to notify Discloser, to the extent permitted, prior to doing so. OpenAI recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor. Customer agrees not to disclose any OpenAI Confidential Information in response to a FOIA request until OpenAI has had reasonable opportunity to review and object as allowed under the applicable law.
- 7.4. [Reserved]

8. Suspension.

- 8.1. Of End User Accounts. If an End User causes, or will cause, a Security Emergency, then OpenAI may request that the Customer temporarily suspend the relevant End User account. If Customer fails to promptly temporarily suspend or terminate the End User account, then OpenAI may do so.
- 8.2. Of the Services. OpenAI may limit or suspend Customer's access to the Services for so long as reasonably necessary to address the condition given rise to the suspension if: (a) it is required to do so by law; or (b) doing so is necessary to prevent or terminate a Security Emergency. OpenAI will use reasonable efforts to notify Customer before limiting to or suspending the Services pursuant to the preceding sentence but may do so without prior notice to the extent reasonably necessary. OpenAI will use reasonable efforts to: (i) narrowly tailor a limitation or suspension to prevent or terminate the Security Emergency; and (ii) cooperate with Customer to promptly restore access to the Services once it verifies Customer has resolved the condition requiring suspension.

9. IP Rights.

- 9.1. Reservation of Rights. Except as expressly set forth herein, the Agreement does not grant: (a) OpenAI any IP Rights in Customer Content; or (b) Customer any IP Rights in the Services. Customer obtains only a limited right to use the Services, and no ownership rights are transferred to Customer or its End Users under this Agreement.
- 9.2. Limited Permission. Customer grants OpenAI only the limited rights that are reasonably necessary for OpenAI to deliver the Services. This limited permission also extends to subcontractors or sub-processors.

9.3. Feedback. If Customer provides Feedback, Customer grants OpenAI the right to use and exploit Feedback without restriction or compensation. OpenAI acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

10. No Publicity. Except with express prior written permission in each instance, neither Party will: (i) include the other Party's name or logo on their websites, media, or marketing materials; or (ii) make any public statement about its relationship with the other Party or this Agreement.

11. Term and Termination.

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

11.2. Termination. When the End User is an instrumentality of the United States, recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, OpenAI shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

11.3. Effects of Termination. If this Agreement terminates: (a) the rights granted by OpenAI to Customer will cease immediately; and (b) OpenAI will delete all Customer Content from its systems within thirty days, unless: (i) OpenAI is legally required to retain it; or (ii) Customer has agreed otherwise in writing. Termination or expiration will not affect any rights or obligations, including the payment of amounts due, which have accrued under this Agreement up to the date of termination. Despite anything to the contrary in this Agreement, OpenAI may retain Abusive Customer Content, or, if Customer's access to the Services is suspended via Section 8 or terminated via Section 11, share information related to Abusive Customer Content, as required by law, or as reasonably necessary to protect the Services or any third party from harm.

11.4. Survival. The following provisions will survive termination or expiration of the Agreement: 6.2 (Payment), 7 (Confidentiality), 9 (IP Rights), 11.3 (Effects of Termination), 11.4 (Survival), 12 (Warranties; Disclaimers), 13 (Indemnification), 14 (Limitation of Liability), 16 (Miscellaneous).

12. Warranties; Disclaimer.

12.1. Warranties. OpenAI warrants that, during the Term, when used in accordance with this Agreement, the Services will conform in all material respects with the Documentation.

12.2. Disclaimer. SUBJECT TO SECTION 12.1, THE SERVICES ARE PROVIDED "AS IS." TO THE EXTENT PERMITTED BY LAW, EXCEPT AS EXPRESSLY STATED IN THE AGREEMENT, OPENAI AND ITS AFFILIATES AND LICENSORS MAKE NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE, OR NON-INFRINGEMENT. OPENAI MAKES NO REPRESENTATION, WARRANTY OR GUARANTEE THAT SERVICES WILL MEET CUSTOMER'S REQUIREMENTS OR EXPECTATIONS, THAT CUSTOMER CONTENT WILL BE ACCURATE, THAT DEFECTS WILL BE CORRECTED, OR REGARDING ANY THIRD-PARTY SERVICES. OPENAI WILL NOT BE RESPONSIBLE OR LIABLE FOR ANY CUSTOMER CONTENT, THIRD-PARTY SERVICES, THIRD-PARTY CONTENT, OR NON-OPENAI SERVICES (INCLUDING FOR ANY DELAYS, INTERRUPTIONS, TRANSMISSION ERRORS, SECURITY FAILURES, AND OTHER PROBLEMS CAUSED BY THESE ITEMS).

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

13. Indemnification.

13.1. By OpenAI. OpenAI agrees to indemnify, defend, and hold Customer harmless against any liabilities, damages and costs (including reasonable attorneys' fees) payable to a third party arising out of a Claim alleging that the Services infringe any third-party IP Right. This excludes claims to the extent arising from: (a) combination of any Services with products, services, or software not provided by OpenAI or on OpenAI's behalf; (b) modification of any Services by any party other than OpenAI; (c) Customer Content; (d) Customer Applications (if any and the claim would not have arisen but for the Customer Application). In addition, the Service-Specific Terms Indemnity, as of the Effective Date, is included in this Agreement, is not subject to any liability cap, and OpenAI may not materially reduce Customer's protections under the Service-Specific Terms Indemnity without Customer's written agreement. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

13.2. [Reserved]

- 13.3. Mitigation. If OpenAI reasonably believes that all or any portion of the Services is likely to become the subject of an infringement Claim, OpenAI will: (a) obtain, at OpenAI's expense, the right for Customer to continue using the Services in accordance with this Agreement; (b) replace or modify the allegedly infringing Service; or (c) if (a) and (b) are not commercially practicable, OpenAI may, in its sole discretion, terminate this Agreement upon written notice to Customer and refund any prepaid amounts for unused Services. Customer will promptly comply with all reasonable instructions provided by OpenAI with respect to the above, including any instruction to replace, modify, or cease use of the Service.
- 13.4. Procedure. A party seeking indemnity will provide the indemnifying party with prompt written notice upon becoming aware of any claim, reasonable cooperation in the defense of or investigation of the claim and allow the indemnifying party control of defense and settlement of the claim including selection of counsel, provided that the party seeking indemnity is entitled to participate in its own defense at its sole expense. The indemnifying party cannot enter any settlement or compromise of any claim without prior written consent of the other party, which will not be unreasonably withheld, except that the indemnifying party may without consent enter any settlement of a claim that resolves the claim without liability to the other party, impairment to any of the other party's rights, or requiring the other party to make any admission of liability. THE INDEMNITIES ARE A PARTY'S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY THE OTHER PARTY OF A THIRD PARTY'S IP RIGHTS.

14. Limitation of Liability.

- 14.1. Limitation on Indirect Liability. TO THE FULLEST EXTENT PERMITTED BY LAW, EXCEPT FOR: (A) A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; (B) CUSTOMER'S BREACH OF SECTION 3.3 (RESTRICTIONS); (C) OPENAI'S BREACH OF SECTION 5.1 (SECURITY MEASURES); OR (D) EITHER PARTY'S BREACH OF SECTION 7 (CONFIDENTIALITY); NEITHER CUSTOMER NOR OPENAI OR EITHER PARTY'S AFFILIATES OR LICENSORS WILL BE LIABLE UNDER THIS AGREEMENT FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING LOST PROFITS, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE.
- 14.2. Limitation on Amount of Liability. TO THE FULLEST EXTENT PERMITTED BY LAW, EXCEPT FOR: (A) A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, (B) A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT, OR (C) CUSTOMER'S PAYMENT OBLIGATIONS, EACH PARTY'S TOTAL LIABILITY UNDER THE AGREEMENT WILL NOT EXCEED THE TOTAL AMOUNT CUSTOMER PAID TO OPENAI DURING THE TWELVE MONTHS IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO LIABILITY. THE FOREGOING LIMITATIONS APPLY DESPITE ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

15. Disputes. All contract disputes shall be resolved in accordance with the Contract Disputes Act, 41 U.S.C. 7101-7109, or other Disputes procedures set forth in the applicable Government contract.

16. Miscellaneous.

- 16.1. Entire Agreement. This Agreement is the entire agreement between Customer and OpenAI with respect to its subject matter and supersedes all prior or contemporaneous agreements, communications and understandings, whether written or oral. This Agreement hereby incorporates by attachment and this reference the OpenAI Policies and relevant Order Forms. Customer agrees that any terms and conditions contained in any purchase order Customer sends to OpenAI will not apply to this Agreement and are null and void.
- 16.2. Conflicting Terms. If there is a conflict between the documents that make up the Agreement, the documents will control in the following order, the: (a) Order Form; (b) Service-Specific Terms; (c) Agreement; and (d) OpenAI Policies.
- 16.3. Governing Law. This Agreement will be governed by the Federal laws of the United States.
- 16.4. Severability. Unenforceable provisions will be modified to reflect the parties' intention and only to the extent necessary to make them enforceable, and the remaining provisions of the Agreement will remain in full effect.
- 16.5. Notices. Notices must be sent via email, first class, airmail, or overnight courier and are deemed given when received. Notices to Customer may also be sent to the applicable Account email address and are deemed given when sent. Notices to OpenAI must be sent to OpenAI Legal at contract-notices@openai.com, with a copy to: (a) if OpenAI, L.L.C., 1455 3rd Street, San Francisco, California 94158; or (b) if OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland.
- 16.6. Waiver. A waiver of any default is not a waiver of any subsequent default.
- 16.7. Assignment. The Agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Customer's prior approval.
- 16.8. No Agency. OpenAI and Customer are not legal partners or agents but are independent contractors.

- 16.9. Force Majeure. In accordance with FAR Clause 52.212-4(f), except for payment obligations, neither Customer nor OpenAI will have any liability for failures or delays resulting from conditions beyond Customer's or OpenAI's reasonable control, including but not limited to governmental action or acts of terrorism, earthquake or other acts of God, labor conditions, or power failures.
- 16.10. No Third-Party Beneficiaries. There are no intended third-party beneficiaries to this Agreement, and it is Customer and OpenAI's specific intent that nothing contained in this Agreement will give rise to any right or cause of action, contractual or otherwise, in or on behalf of any third party.
- 16.11. Trade Controls. Customer is solely responsible for ensuring that its use of the Services complies with applicable trade laws, including sanctions and export control laws. Customer's Input may not include material or information that requires a government license for release or export. Customer may not use the Services in or for the benefit of, or export or re-export the Services to, any U.S. embargoed countries or to anyone on a Restricted Party List. Customer represents and warrants that Customer and End Users are not located in any U.S. embargoed countries, are not identified on any Restricted Party List, and that Customer will comply with applicable export control laws, including any "know your customer" requirements or obligations applicable to Customer's End Users.
- 16.12. Geographical Limitations on Use. Customer and End Users may not access or offer access to the Services outside of the Supported Countries and Territories. A violation of this Section 16.13 may result in Services suspension under Section 8.
- 16.13. Updates.
- a. Generally. OpenAI may non-materially update this Agreement, or OpenAI Policies, by providing Customer with reasonable notice, including by posting the update on OpenAI's website. Any other updates will be effective on the date OpenAI posts the non-materially updated Agreement or OpenAI Policy. Customer's continued use of, or access to, the Services after an update is effective constitutes acceptance of the non-material update. If Customer does not agree with a non-material update, Customer may stop using the Services or terminate this Agreement under Section 11. Any material updates to this agreement shall be presented to Ordering Activity for review and will not be effective unless and until both parties sign a written agreement updating these terms.
 - b. Exceptions. Except for an update to comply with applicable law, updates to this Agreement or the OpenAI Policies will not apply to: (i) Disputes between Customer and OpenAI arising prior to the update; or (ii) Order Forms signed by Customer and OpenAI (as opposed to an automated ordering page) prior to OpenAI notifying Customer of the update. However, to the extent an update relates to a Service or feature launched after an Order Form is signed it will be effective upon Customer's first use of that Service
- 16.14. Government Entity Rights. This Section 16.15 applies to Government Entities. For U.S. federal Government Entities, the Services are "commercial computer software" as defined at 48 C.F.R. § 2.101 and 48 C.F.R. § 252.227-7014(a)(1) and as the term is used in 48 C.F.R. §§ 12.212 and 227.7202, and related services are "commercial services" as defined in 48 C.F.R. § 2.101. The Services and Documentation are: (a) provided to Government Entity Customers and End Users, for use by the Government Entity or on its behalf; (b) subject to this Agreement and with only those rights as are granted to all other Customers and End Users, except to the limited extent prohibited by applicable law.
17. Definitions.
- "Abusive Customer Content" means Inputs or Outputs that violate Section 3.3.
- "Account" means an administrative account provided to Customer by OpenAI for the purpose of administering the Services.
- "Administrator" means a Customer designated End User with administrative privileges.
- "Account Console" means the online tool provided by OpenAI to Customer for use in administering the Services.
- "Affiliate" means with respect to either Party, any other person or entity that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with, that Party.
- "API" means OpenAI's application programming interface.
- "Audit Reports" means the third-party audit reports for the Services.
- "Authorized Purchaser" means a Customer employee designated by Customer to act as an authorized purchaser of the Services. Customer can designate Authorized Purchasers in an offline Order Form or in the Admin Console. Administrators are Authorized Purchasers. Authorized Purchasers may be periodically updated by Customer in the Account Console.
- "Batch" means, for purposes of Section 15.7, a group of up to 50 claimants.
- "Beta Services" means services or features identified as alpha, beta, preview, early access, or evaluation, or words or phrases with similar meanings.

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

“Claim” means legal proceedings filed by a third party.

“Customer Application” means Customer’s applications, products, or services that integrate with an OpenAI API. “Customer Content” means the Input and the Output.

“Discloser” means the Party that discloses Confidential Information to the other under this Agreement. “Dispute” means a claim by a Party arising out of or relating to this Agreement or the Services.

“Documentation” means the documentation OpenAI provides to Customer or otherwise makes publicly available. “DPA” means the OpenAI data processing addendum attached hereto and at: <https://openai.com/policies/data-processing-addendum/>.

“Effective Date” means the date this Agreement is entered into by the Parties, either by signing an Order Form referencing the Agreement, or by signing the Agreement itself.

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

“End User Account” means an account for an End User under Customer’s Account. “Feedback” means any feedback provided by Customer to OpenAI regarding the Services.

“Fees” means all fees charged to Customer’s Account in accordance with an Order Form.

“Governing Laws” means: (a) for Customers in the EEA, Switzerland, or UK, the laws of Ireland; and (b) for all other Customers, the laws of the State of California, excluding California’s conflicts of law rules or principles.

“Government Entity” means any nation or government, any state, municipality, or other political subdivision thereof, and any entity, body, agency, commission, department, board, bureau or court, whether domestic, foreign or multinational, exercising executive, legislative, judicial, regulatory or administrative functions of or pertaining to government, and any employee or official thereof.

“Healthcare Addendum” means the OpenAI Healthcare Addendum and Business Associate Agreement provided by OpenAI to Customer.

“Informal Dispute Resolution Form” means the form located at [this link](#).

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

“Input” means Customer and Customer’s End Users input to the Services.

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

“NAM” means National Arbitration and Mediation.

“OpenAI Contracting Party” means: (a) OpenAI OpCo, LLC for Customers located outside the EEA or Switzerland; (b) OpenAI Ireland Ltd. for Customers located in the EEA or Switzerland; or (c) OpenAI Public Sector, LLC if designated on the Order Form.

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

“Order Form” means: (a) when purchasing from OpenAI, the ordering document signed by Customer and OpenAI or OpenAI webpage that Customer uses to purchase the Services; or (b) when purchasing from a reseller, the ordering document signed by Customer and its reseller or reseller’s webpage Customer uses to purchase the Services.

“Output” means output from the Services based on the Input.

“Permitted Exception” means Customer using Output to: (a) develop artificial intelligence models primarily intended to categorize, classify, or organize data (e.g., embeddings or classifiers), if these models are not distributed or made commercially

available to third parties; and (b) fine tune or customize models provided as part of OpenAI's fine-tuning or other Services set forth on the Pricing Page.

"Personal Data" is as defined in the DPA.

"Pricing Page" means the pages available at <https://openai.com/api/pricing/> or <https://openai.com/chatgpt/pricing/>. "Protected Health Information" is as defined under the HIPAA Privacy Rule (45 C.F.R. Section 160.103).

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

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

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

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

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

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

"Service Credits" means, for the Services, either credits purchased by Customer or promotional credits provided by OpenAI to Customer.

"Service Credit Terms" means the terms available at: <https://openai.com/policies/service-credit-terms/>.

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

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

"Service-Specific Terms" means the terms specific to certain services attached hereto and at:

<https://openai.com/policies/service-terms>.

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

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

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

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

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

"Third-Party Services" means products, services, or content offered by parties other than OpenAI through the Services.

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

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

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



OpenAI Government Addendum

This OpenAI Government Addendum (“Government Addendum”) to the OpenAI Services Agreement (the “Agreement”) is made by and between OpenAI Public Sector, LLC and Customer. Capitalized terms not defined in this Government Addendum have the meanings provided in the Agreement or applicable Order Form. This Government Addendum amends and supplements the Services Agreement, as expressly set forth herein, and forms part of the Agreement.

The Parties acknowledge that certain terms in the Agreement are inconsistent with procurement laws and regulations and are, therefore, modified as provided below.

1. Preamble. The Agreement shall bind the Government as Customer and End User but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.
2. Automatic Renewal. No Service provided under the Agreement shall renew automatically upon expiration of its current term without prior express consent by an authorized Government representative.
3. Modifications. No material reduction in Services will take effect on the Government without prior express consent by an authorized Government representative.
4. Taxes. Any taxes or surcharges which OpenAI seeks to pass along to the Government will be governed by the terms of any applicable underlying Government contract and, in any event, must be submitted to the Government for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the applicable underlying government contract.
5. Disputes. All contract disputes shall be resolved in accordance with the Contract Disputes Act, 41 U.S.C. 7101-7109, or other Disputes procedures set forth in the applicable Government contract.
6. Confidentiality. OpenAI recognizes that governments may be subject to open information laws, such as the Federal Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released publicly. Customer agrees not to disclose any OpenAI Confidential Information in response to a FOIA request until OpenAI has had reasonable opportunity to review and object as allowed under the applicable law.
7. Suspension of the Services. Any suspension of the Services for a Customer violation of the Agreement or OpenAI Policies will be subject to the Disputes section of this Government Addendum (Section 5 above).
8. Termination. Any Termination by OpenAI will be subject to the Disputes section of this Government Addendum (Section 5 above).

9. Indemnification by OpenAI. With respect to any indemnification by OpenAI, OpenAI acknowledges that the U.S. Department of Justice, or other equivalent government department, has the sole right to represent the government in litigation.
10. Indemnification by Customer. Any term in the Agreement requiring the Customer to indemnify OpenAI is deleted. Customer represents and warrants that:
 - (a) it will not use the Services in violation of the Agreement;
 - (b) any Customer Applications made available in connection with the Services will not give rise to any third-party claims against OpenAI or its affiliates and licensors; and
 - (c) Customer Content will not infringe upon, misappropriate, or otherwise violate any rights of any third party or give rise to any third-party claims against OpenAI or its affiliates and licensors.
11. Arbitration. Any term in the Agreement requiring arbitration is deleted.
12. Governing Law and Venue. The Agreement will be governed by Federal law or other law applicable to Customer, and any action shall be brought in a venue authorized by such law.
13. Assignment. The Agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Customer's prior approval.

This OpenAI FedRAMP Addendum (this “Addendum”) supplements the Order Form that references this Addendum (the “Order Form”) by and between the OpenAI entity (“OpenAI”) and the customer (“Customer”) listed in the Order Form and applies to the FedRAMP Environment only. Capitalized terms not defined in this Addendum shall have the meanings ascribed to them in the OpenAI Services Agreement located at <https://openai.com/policies/services-agreement/> (“Agreement”).

1. FedRAMP Environment Accreditation. As of the execution date, OpenAI maintains the FedRAMP accreditations identified at <https://marketplace.fedramp.gov/products> for the FedRAMP Workspace and FedRAMP Organization. OpenAI intends to, and will make commercially reasonable efforts to, maintain these accreditations for the duration of the Agreement.
2. Data Residency. When Customer uses the FedRAMP Environment, OpenAI performs all model inference, and permanently stores all Customer Content at rest, within the United States. The foregoing commitments do not apply with respect to: (a) any transient storage or routing of encrypted Customer Content outside of the US necessary to provide the Services; (b) Third Party Offerings; (c) any data other than Customer Content, such as System Data, or (d) computational processing of Customer Content outside the US for orchestration, indexing, and analytics.
3. Limitations. Customer agrees that this Addendum only applies to newly created FedRAMP ChatGPT Workspaces and FedRAMP API Organizations after the execution of the Order Form. If Customer has an existing non-FedRAMP ChatGPT Workspace or API Organization, the commitments in this Addendum will not apply. Customer acknowledges that Customer’s access to newly released features of the Services may be delayed or limited in order to meet the requirements of this Addendum.
4. FedRAMP Compliance. Other than providing the FedRAMP Environment in accordance with this Addendum, OpenAI does not assume responsibility for Customer’s compliance with FedRAMP or any other federal, state, or regulatory requirements. Customer is solely responsible for determining whether its use of the Services meets its applicable compliance obligations and for implementing and maintaining any administrative, technical, or operational controls required for such compliance.
5. ChatGPT Enterprise. When using ChatGPT Enterprise within a FedRAMP Workspace, all End Users must be internal only (e.g., employees, contractors, agents, affiliates) and must be authenticated via Single Sign-on (SSO).
6. API Terms. When using API Services within a FedRAMP Organization, Customer will comply with the following requirements:
 - 6.1. Access FedRAMP accredited API models at gov.api.openai.com
 - 6.2. If the Customer Application consists of a chat or conversation application, Customer will ensure the Customer Application responses are restricted by topic or grounded in trusted documents or files (e.g., no general purpose chat functions);
 - 6.3. Any End Users that generate content that is provided as Input to the Services will be internal only (e.g., employees, contractors, agents, affiliates) or will be authenticated using one of the following mechanisms: (a) 2 factor/multi-factor authentication; (b) single sign-on; or (c) user ID and password where logins are logged for visibility and remediation;
 - 6.4. Customer will perform moderation by implementing OpenAI’s ModAPI or an alternative moderation tooling and will notify OpenAI and discuss in good faith if Customer detects notable spikes on high severity abuse;
 - 6.5. If Customer uses the Services to generate code: (a) Customer will limit code generation to internal End Users or, where external End User use a Customer Application for code generation, implement monitoring for misuse; and (b) require a human-in-the-loop to review code before it is launched in production;
 - 6.6. If the Customer Application permits End Users to upload images as Inputs, limit the image inputs to low risk and/or topical documents.

7. Definitions.

“FedRAMP Environment” means the OpenAI environment that has received a FedRAMP authorization and includes the FedRAMP Workspace and FedRAMP Organization.

“FedRAMP Organization” means a preconfigured ChatGPT API organization within the FedRAMP Environment that has received FedRAMP accreditation and is accessible at gov.api.openai.com.

“FedRAMP Workspace” means a preconfigured ChatGPT Enterprise workspace within the FedRAMP Environment that has received FedRAMP accreditation

“System Data” means account data, metadata, and usage data, to the extent each does not contain Customer Content, that is collected by the Services and used to manage and operate the Services, including, without limitation, End User account information, End User profiles, analytics, usage statistics, billing information, support requests.

“Third Party Offering” means products, services, or content offered by third parties on the Services or integrated with the Services.

OpenAI Data Processing Addendum

This OpenAI Data Processing Addendum (“DPA”) supplements, and is incorporated into, the OpenAI Services Agreement (“Agreement”) governing use of the Services and is entered as of the Effective Date between the customer identified above (“Customer”) and OpenAI OpCo, LLC, on its behalf and on behalf of its Affiliates, as appropriate, unless Customer is based within a European Economic Area country or Switzerland, in which case it is entered into with OpenAI Ireland Ltd., on its behalf and on behalf of its Affiliates, as appropriate (“OpenAI”). Capitalized terms not defined in the DPA have the meanings provided in the Agreement. In this DPA, OpenAI and Customer are each referred to as a “Party” and collectively as the “Parties.” Customer represents it is lawfully able to enter into this Agreement and, if it is entering into the Agreement for an entity, that it has legal authority to bind that entity. By accepting the Order Form, , Customer agrees to this Agreement.

1. Details.

- 1.1. Scope and Roles. As part of providing the Services to the Customer under the Agreement, OpenAI may Process Customer Data on behalf of Customer. OpenAI acts as a Data Processor on the Customer’s behalf, and this DPA governs such Processing.
- 1.2. Details of Processing. OpenAI will only Process Customer Data for the purposes of delivering the Services to Customer pursuant to the Agreement and this DPA. Details regarding the nature, duration, as well as the types of Customer Data and categories of Data Subjects involved, are set out in Schedule 1 (Details of Processing) to this DPA. OpenAI and Customer each agree to comply with their respective obligations under Data Protection Laws in connection with the Services.

2. OpenAI Obligations.

- 2.1. Customer Instructions. The Parties agree that this DPA, the Agreement (including the Order Form), and any instructions provided via the configuration tools and other tools within the Services made available by OpenAI within the Services, constitute Customer’s documented instructions regarding OpenAI’s processing of Customer Data (“Customer Instructions”). OpenAI will process Customer Data only in accordance with Customer Instructions, unless required to do so by applicable law to which OpenAI is subject, in which case OpenAI will inform Customer of this requirement prior to processing unless legally prohibited from doing so.
- 2.2. Notices to Customer. OpenAI will promptly inform Customer in writing if, in OpenAI’s opinion, a Customer Instruction violates Data Protection Laws. OpenAI will, to the extent legally permitted, inform Customer if OpenAI receives a legally binding request for disclosure of Customer Data by a law enforcement authority.
- 2.3. Confidentiality. OpenAI will ensure that all persons authorized by OpenAI to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 2.4. Data Subject Requests. OpenAI will, to the extent legally permitted, inform Customer if OpenAI receives a request to exercise data subject rights pursuant to Data Protection Laws (“Data Subject Request”) in respect of Customer Data. OpenAI will not respond to any such request without Customer’s prior written authorization, except that Customer authorizes OpenAI to redirect Data Subject Requests as necessary to allow Customer to respond directly. Taking into account the nature of the processing, OpenAI will assist Customer by implementing appropriate technical and organizational measures, in so far as this is possible, to allow Customer to respond to Data Subject Requests.
- 2.5. Security. OpenAI will implement and maintain reasonable and appropriate organizational and technical security measures to protect Customer Data, as set forth in the Agreement.
- 2.6. Assistance to Customer. OpenAI will, taking into account the nature of the processing and the information available to OpenAI, provide reasonable assistance to Customer to help Customer comply with its obligations under Data Protection Laws including, where appropriate, the preparation of data protection impact assessments with respect to OpenAI’s processing of Customer Data and, where necessary, the Customer consulting with a supervisory authority with jurisdiction over such processing, if such consultation is required by Data Protection Laws.
- 2.7. Personal Data Breaches. OpenAI will notify Customer without undue delay, but no later than seventy-two (72) hours after becoming aware of any Personal Data Breach. OpenAI will provide reasonable assistance to Customer to help Customer comply with its obligations under Data Protection Laws in respect of such Personal Data Breach.
- 2.8. Assessing Compliance. OpenAI will, on Customer’s reasonable written request and to the extent required by Data Protection Laws: (i) no more than once per year, provide Customer with OpenAI’s privacy and security policies and other such information necessary to demonstrate compliance with OpenAI’s obligations under this DPA; and (ii) provided that the Parties have an appropriate confidentiality agreement in place, allow for and contribute to audits

or inspections by, or on behalf of, Customer at Customer's sole expense. Such audit or inspection must be: (A) conducted in a manner that is minimally disruptive to OpenAI's business; (B) necessary to confirm that OpenAI is processing Customer Data in a manner consistent with this DPA; and (C) occur no more than once per year. Where permitted by Data Protection Laws, OpenAI may instead make available to Customer a summary of the Audit Reports relevant to OpenAI's compliance with this DPA. Such results and documentation, including the results of any audits or inspections, shall be the Confidential Information of OpenAI.

- 2.9. Engagement of Sub-processors. Customer hereby provides a general authorization to OpenAI to engage the Sub-Processors listed in the Sub-Processor List to process Customer Data in connection with the Services. OpenAI will notify Customer of any changes to the Sub-Processor List via blog post, notification within the Services or other reasonable means, or via email if Customer subscribes to email notifications on the Sub-Processor List site. Customer may object to the use of such additional Sub-processor within 30 days of receiving notice of the change by following the instructions set forth in the Sub-Processor List or by contacting privacy@openai.com. In such case, OpenAI will work with Customer to address its concerns and offer commercially reasonable alternatives or solutions. If none of the alternatives or solutions are commercially feasible, in OpenAI's reasonable judgment, or if the objections have not been resolved to the satisfaction of the Parties within 30 days of OpenAI's receipt of Customer's objection notice, then either Party may terminate the Agreement or any Order Forms or usage regarding the Services that cannot be provided without the use of the new Sub-Processor. In such case, Customer will be refunded any applicable pre-paid fees to the extent they cover periods or terms following the date of such termination.
- 2.10. Sub-processor obligations. OpenAI shall enter into contractual arrangements with each Sub-Processor that imposes on them obligations comparable to those imposed on OpenAI under this DPA. Subject to the limitations of liability included in the Agreement, OpenAI will remain liable for the acts and omissions of its Sub-Processors to the same extent OpenAI would be liable under this DPA if it performed such acts or omissions itself.
- 2.11. Data Return or Deletion. Following expiry or termination of the Agreement, OpenAI will, at Customer's instruction, return or delete Customer Data, and existing copies unless retention of Customer Data is required under applicable laws, in which case OpenAI will isolate and protect it from any further processing except to the extent required by applicable laws.

3. Customer Obligations.

- 3.1. Notices and authorizations. Customer represents, warrants and covenants that it has provided all necessary notices, and has and shall maintain throughout the Term all necessary rights, consents and authorizations, to the extent required under Data Protection Laws, to provide the Customer Data to OpenAI and to authorize OpenAI to process Customer Data in connection with the Agreement, including this DPA.
- 3.2. Cooperation. Customer shall reasonably cooperate with OpenAI to assist OpenAI in performing any of its obligations under applicable Data Protection Laws.
- 3.3. Configurations. Without prejudice to OpenAI's security obligations in Section 2.5 of this DPA, Customer acknowledges and agrees that it is responsible for certain configurations and design decisions for the Services and for implementing such configurations and design decisions (e.g., retention periods, deletion, etc.) in a manner that complies with applicable Data Protection Laws.

4. International Data Transfers.

- 4.1. EEA and Swiss Data. Customer Data processed by OpenAI under this DPA may fall within the scope of the Data Protection Laws of the European Economic Area or Switzerland ("EEA and Swiss Data"). Regardless of the OpenAI applicable contracting Party under this DPA, Customer hereby instructs OpenAI Ireland Limited to process any EEA and Swiss Data in compliance with this DPA. To the extent OpenAI Ireland Limited transfers EEA and Swiss Data to other OpenAI Affiliates or third parties outside the European Economic Area or Switzerland to provide the Services, it will do so on the basis of agreements containing SCCs that ensure appropriate safeguards for the protection of Customer Data are in place or an adequacy decision issued by the European Commission under Article 45 GDPR.
- 4.2. UK Data. Customer Data processed by OpenAI under this DPA may fall within the scope of the Data Protection Laws of the United Kingdom ("UK Data"). Regardless of the OpenAI applicable contracting Party under this DPA, Customer hereby instructs OpenAI OpCo, LLC to process any UK Data in compliance with this DPA and with the SCCs as amended by the UK Addendum, which are deemed entered into (and attached hereto and incorporated into this DPA by this reference) and completed as described in Schedule 1.

5. Further Requirements. To the extent U.S. Privacy Laws apply:

- 5.1. OpenAI agrees to (a) not provide Customer with monetary or other valuable consideration in exchange for Customer Data from Customer. The parties acknowledge and agree that Customer has not "sold" (as such term is defined by

U.S. Privacy Laws) Customer Data to OpenAI; (b) not “sell” (as such term is defined by U.S. Privacy Laws) or “share” (as such term is defined by the CCPA) Personal Data; (c) to the extent that Customer permits or instructs OpenAI to process Customer Data subject to U.S. Privacy Laws in a de-identified form as part of the Services, OpenAI shall (i) adopt reasonable measures to prevent such deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) publicly commit to maintain and use such deidentified data in that form and not attempt to re-identify the information, except as may be permitted by U.S. Privacy Laws; and (iii) before sharing de-identified data with any other party, including Sub-Processors, contractually obligate any such recipients to comply with the requirements of this provision (c)(i)-(iii); and (d) where the Customer Data is subject to the CCPA (i) not retain, use, disclose, or otherwise process Customer Data except as necessary for the business purposes specified in the Agreement, including without limitation as set out in Schedule 1 of this DPA; (ii) not retain, use, disclose, or otherwise process Customer Data in any manner outside of the direct business relationship between OpenAI and Customer; (iii) not 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; (iv) notify Customer without undue delay if OpenAI determines that it can no longer meet its obligations under the CCPA; and (v) if Customer reasonably believes that OpenAI’s Processing of Customer Data is not consistent with the requirements of the CCPA and upon Customer’s reasonable notification of the same to OpenAI, the Parties will work together in good faith to remedy the issue, or, if after working together Customer reasonably determines that the issue cannot be remedied, OpenAI will stop Processing the affected Customer Data upon written instruction from Customer.

- 5.2. Customer agrees to not take any action that would (a) render the provision of Customer Data to OpenAI a “sale” under U.S. Privacy Laws or a “share” under the CCPA (or equivalent concepts under U.S. Privacy Laws); or (ii) render OpenAI not a “service provider” under the CCPA or “processor” under U.S. Privacy Laws.

6. Definitions.

“Customer Data” means Personal Data processed by OpenAI on behalf of Customer to provide the Services.

“Data Controller” has the meaning assigned to the term “controller” (or another analogous term) under Data Protection Laws.

“Data Processor” has the meaning assigned to the term “processor” (or another analogous term) under Data Protection Laws.

“Data Protection Laws” means data privacy and data protection laws applicable to OpenAI’s processing of Customer Data in connection with the Services.

“Data Subject” has the meaning assigned to the term “data subject” (or another analogous term) under Data Protection Laws.

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

“Personal Data” has the meaning assigned to the term “personal data” or “personal information (or another analogous term) under Data Protection Laws.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data stored, transmitted or otherwise processed by OpenAI, its Sub-Processors, or any other third parties acting on OpenAI’s behalf.

“Processing” has the meaning assigned to the term “processing” (or another analogous term) under Data Protection Laws.

“SCCs” means the standard contractual clauses for the transfer of personal data to third countries adopted by the EU Commission on June 4, 2021 (as may be amended, updated or replaced from time to time).

“Sub-Processors” means the sub-processors engaged by OpenAI to process Customer Data in connection with the Services, listed in the Sub-Processor List.

“Sub-Processor List” means the list available at the following address <https://platform.openai.com/subprocessors>.

“UK Addendum” means the UK addendum to the EU SCCs issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018, attached hereto and available at <https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf>.

“U.S. Privacy Laws” means the subset of Data Protection Laws applicable to residents of the United States, including without limitation the California Consumer Privacy Act (“CCPA”).

Schedule 1 Details of Processing

1. Nature and Purpose:

The performance of the Services under the Agreement.

2. Duration:

The Term and such time required thereafter for the Parties to perform their applicable obligations following the end of the Term, including data deletion.

3. Categories of Customer Data:

Customer may submit Personal Data to the Services, the categories of which will depend upon Customer's use of the Services which is determined and controlled by Customer in its sole discretion, but it may include, but is not limited to names, contact information, demographic information, or any other information provided by Customer's End Users in unstructured data.

4. Categories of data subjects:

The data subjects may include, but are not limited to Customer's employees, customers, suppliers and generally End Users.

5. Sensitive data transferred (if applicable):

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

6. Frequency:

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

Continuous basis depending on Customer's use of the Services

7. Transfers to Sub-Processors:

As per Article 2.9 of the DPA, Sub-Processors will Process Customer Data as necessary to perform the Services. Such Processing will be for the duration of the Agreement, unless otherwise agreed in writing.

8. SCCs information for the transfer of UK Data under Section 4.2:

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

8.2. For each module of the SCCs, where applicable, the following applies: (i) The optional docking clause in Clause 7 does not apply; (ii) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 2.9 of the 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 SCCs will be governed by the laws of England and Wales; (vi) In Clause 18(b), disputes will be resolved before the courts of England and Wales; (vii) This Schedule 1 contains the information required in Annex I and Annex III of the SCCs; (viii) Section 2.5 (Security) of the DPA contains the information required in Annex II of the SCCs, (ix) the competent supervisory authority is the Information Commissioner's Office ("ICO").

8.3. Data exporter(s): the Customer under the Agreement; Data importer(s): OpenAI OpCo, LLC, 1455 3rd Street, San Francisco, CA 94158, Data Protection Officer, privacy@openai.com.

[Execute Data Processing Agreement](#)

Terms and Conditions for LLM Developers' Government Addendum

(a) *Applicability*

- (1) These terms and conditions apply when Government Data will be processed by a Large Language Model Artificial Intelligence System (LLM).
- (2) These terms and conditions do not apply when—
 - (i) The LLM is embedded in a common commercial product, such as a word processor or map navigation system (see Section 7223(4)(B) of Pub. L. 117-263);
 - (ii) The LLM functionality is incidental to the primary purpose of the core requirement being procured.

(b) *Definitions.* As used in these terms and conditions —

Background Data means any pre-existing proprietary content, reference materials, knowledge bases, or other intellectual property owned or controlled by the LLM Developer that may be referenced, retrieved, augmented, or otherwise incorporated into the LLM's processing or outputs through any enrichment mechanism, including but not limited to retrieval processes, vector stores, embeddings, knowledge graphs, plugins, tool calls, agent actions, or similar mechanisms.

Custom Development means any design of or modifications, customizations, configurations, or enhancements to LLMs or associated implementations or workflows, and any related work product or deliverables, in each case developed specifically for the Government under this contract or task/delivery order, including any modifications, customizations, configurations, or enhancements to LLMs as a result of model training or fine-tuning. Custom Development excludes any background intellectual property (e.g., the underlying supporting services, default configurations, and/or mechanisms) existing prior to entry into this contract or developed independently by the LLM Developer.

Data has the same meaning as defined in 44 U.S.C. §3502(16) and must, without limiting the generality of the foregoing, specifically include Data Inputs and Data Outputs.

Data Inputs means all data, information, personally identifiable information (PII), or content submitted to the LLM and related operational systems by, or created for, the Government, including but not limited to user prompts, queries, instructions, system prompts, source data, documents, knowledge bases, Government email addresses, user account information, and any other information or content submitted to the LLM and related operational systems by or on behalf of the Government. This definition specifically excludes any background intellectual property or information existing prior to entry into this contract or task/delivery order or developed independently by such LLM Developer.

Data Outputs means all data, information, PII, any improvements, enhancements, corrections, annotations, or other modifications made to Data Inputs, or content generated by the LLM in the performance of this contract in response to Data Inputs, including but not limited to responses, results, analyses, anonymized data, derivative data, synthetic data, and any other output produced by the LLM. This definition specifically excludes technical system-level data that contains no Government information or Government usage context, such as performance metrics, token counts, and processing times; technical system-level generated information, such as metadata, logs, and system actions; and any underlying Background Data and third-party proprietary data.

Government means any entity authorized to obtain procurement services through GSA pursuant to 40 U.S.C. § 501, 502.

Government Data means Data Inputs and Data Outputs.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

Large Language Model Artificial Intelligence System (LLM) means a generative artificial intelligence model trained on vast, diverse datasets that enable the model to generate natural-language responses to user prompts (Ref. Executive Order 14319 Section 2). LLM includes the integrated technical and operational environment in which the model is configured, deployed, operated, monitored, or made available for the processing of Government Data, including the model, hosting and access infrastructure, system prompts, configurations, knowledge bases, retrieval mechanisms, Application Programming Interfaces (APIs), user interfaces, guardrails, monitoring systems, and associated workflows.

LLM Developer means the party that performs LLM Development Tasks (as defined in NIST AI RMF 1.0, Appendix A as “AI Development Tasks”) by designing, developing, training, fine-tuning, calibrating, testing, publishing, licensing, or otherwise making available an LLM, including model weights, interfaces, model cards, safety documentation, or conditional usage restrictions. LLM Developer maps primarily to the "AI Development" actor category in NIST AI RMF 1.0, Appendix A.

LLM Service Provider means the party that performs LLM Deployment and Operation & Monitoring (as defined in NIST AI RMF 1.0, Appendix A as “AI Deployment and Operation & Monitoring”) tasks by providing an LLM-enabled application, product, service, workflow, API, user interface, or business capability to Customers or End Users, and controlling the manner in which the service is presented, accessed, administered, supported, or used within that application or workflow. LLM Service Provider maps primarily to the "AI Deployment" and "Operation and Monitoring" actor categories in NIST AI RMF 1.0, Appendix A.

LLM System Integrator means the party that performs LLM Design and LLM Deployment (as defined in NIST AI RMF 1.0, Appendix A as “AI Design” and “AI Deployment”, respectively) tasks by selecting, configuring, adapting, or materially controlling how an LLM System performs in a specific deployment or use case, including by selecting models, setting system prompts, prompt templates, Retrieval-Augmented Generation (RAG) sources, fine-tuning data, tools, plugins, agents, guardrails, filters, evaluation criteria, human-review thresholds, or output constraints. LLM System Integrator maps primarily to the "AI Design" and "AI Deployment" actor categories in NIST AI RMF 1.0, Appendix A, and includes parties NIST identifies as "system integrators."

LLM System Operator means the party that performs LLM Deployment and Operation & Monitoring (as defined in NIST AI RMF 1.0, Appendix A as “AI Deployment and Operation & Monitoring”) tasks by hosting, serving, operating, or providing access to an LLM or LLM System, including through cloud infrastructure, model endpoints, runtime environments, API availability, capacity management, logging, retention, and runtime security. LLM System Operator maps primarily to the "AI Deployment" and "Operation and Monitoring" actor categories in NIST AI RMF 1.0, Appendix A, and may also be a "Third-party entity" where it provides such services for another organization.

Material Change means any modification that could affect the trustworthiness, security, or operational integrity of the performance of the contract, especially as they pertain to the processing and protection of Government Data and the contractors involved in that process.

Personally Identifiable Information (PII) has the same meaning as defined in OMB Circular No. A-130.

- (c) *Order of Precedence*. These terms and conditions establish specific requirements that take precedence over any conflicting provisions in the LLM Developer policies, requirements, terms, conditions, or commercial agreements.
- (d) *LLM Developer Responsibility for LLM*. The LLM Developer must:
 - (1) Exercise due diligence in overseeing the development of the model and performing the activities of an LLM Developer.
 - (2) Notify the Contracting Officer, within 72 hours, of any known violation of a material requirement of this Addendum.
 - (3) The LLM Developer will:
 - (i) Include applicable requirements from these terms and conditions in agreements with LLM Developer(s), System Operator(s), System Integrator(s), and Service Provider(s) when performing services under government contracts; or
 - (ii) Obtain attestation when requested by the government, from an individual with appropriate authority representing LLM's Developer(s), System Operator(s), System Integrator(s), and Service Provider(s) who are partners with the LLM Developers in performing services under government contracts, that requirements have been implemented and provide a new attestation if their compliance changes.
- (e) *Intellectual Property Rights*.
 - (1) *Rights in Government Data*.
 - (i) The Government retains full ownership of, and will own, all Government Data and Custom Developments. The LLM Developer does not have any rights to use Government Data or Custom Developments other than those described in paragraph (e)(1)(iii).
 - (ii) Only LLM Developers, LLM System Operators, LLM System Integrators, and LLM Service Providers who are partners with the LLM Developers in performing services under government contracts may receive and process Government Data.
 - (iii) The LLM Developer is granted a limited, revocable, non-exclusive, non-transferable, worldwide, fully paid-up, royalty-free right and license to copy, store, transmit, modify, display, and use Government Data and Custom Developments for the duration of each individual awarded contract or task/delivery order solely for the following permitted purposes:
 - (A) Performing the specific requirements;
 - (B) Providing technical support and maintenance as required; and
 - (C) Providing such other uses as may be expressly authorized in writing by the Contracting Officer.
 - (iv) To the extent the LLM Developer obtains any intellectual property rights in Government Data, or

any improvements, enhancements, feedback, or derivative works thereof, the LLM Developer assigns and transfers all such rights to the Government effective immediately upon creation.

(v) The LLM Developer retains ownership of the underlying LLM, base models, and Background Data in its original form.

(2) *License Grant to Government.* The LLM Developer grants to the Government an irrevocable, royalty-free, non-exclusive license to use the LLM for the duration of the work defined in the contract or task/delivery order. This license is strictly limited to the specific purposes and scope of work defined within the contract or task/delivery order, and is restricted to the commercially available features, Background Data, and functionality of the LLM as described in and necessary to fulfill this contract or task/delivery order and its accompanying documentation, unless specified otherwise. This license includes the right to:

- (i) Operate and access the LLM through agreed-upon methods;
- (ii) Allow authorized Government personnel and contractors to use the LLM; and
- (iii) Integrate the LLM with Government systems as necessary.

(3) *Prohibited Uses of Government Data.* Use of Government data is limited per paragraph (e)(1)(iii). Other uses of Government data are prohibited. Examples of prohibited use of Government Data includes:

- (i) Training, fine-tuning, or otherwise improving an LLM, including those operated by third parties, or to develop or improve the LLM(s) for any other customers or any commercial or non-commercial purposes.
- (ii) Using Government Data to inform the LLM Developer's advertising, marketing, sales, monetization, strategy, operations, or other business decisions, or to provide to other Government or non-Government entities.
- (iii) Retaining, accessing, or using beyond the scope and duration expressly permitted in the contract.
- (iv) Processing or storing Government Data with, or transferring Government Data to, any party not authorized under this contract or task/delivery order or without appropriate extension (flowdown) of applicable requirements.
- (v) Selling or licensing Government Data to any party.

(4) *Government Data Handling and Processing Requirements.* Unless otherwise expressly authorized by the Contracting Officer:

- (i) The LLM Developer must implement reasonable technical, administrative, physical, and organizational safeguards to protect Government Data from loss, damage, destruction, unauthorized alteration, or corruption, and prevent its unauthorized, accidental, or unlawful access, disclosure, use, or processing;
- (ii) The LLM Developer must implement Data Handling Procedures that restrict human access to Government Data. These protocols must be implemented at the contract level and customization at the individual contract or task/delivery order level. The LLM Developer must implement Automated processing systems and operational controls that prevent human personnel from the LLM Developer or any Third-party entity from viewing, accessing, or reviewing Government Data during normal operations and minimally include:

- (A) Automated data ingestion, processing, and response generation without human content review;
- (B) Technical access controls that prevent personnel from viewing Government Data;
- (C) Encrypted data transmission and processing that renders Government Data unreadable to human personnel;
- (D) Administrative and technical safeguards that allow system operation, monitoring, and maintenance without exposing Government Data content; and
- (E) Audit logging systems that track data processing activities without capturing or displaying actual Government Data.

(iii) The LLM Developer must ensure Government Data is stored or processed only when reasonably necessary for the performance of the contract;

(iv) The LLM Developer must provide tools that enable the Government to maintain detailed records of all processing activities involving Government Data;

(v) The LLM Developer must comply with the following Data localization requirements, including but not limited to:

- (A) Not removing or allowing removal of any such Government Data from the agreed-upon premises or FedRAMP-authorized services, without express written consent from the Contracting Officer; and
- (B) Not transmitting, storing, taking, or accessing such Government Data, or allowing such Government Data to be transmitted, stored, taken, or accessed by any means outside of the agreed-upon premises or authorized services, without express written consent from the Contracting Officer.

(vi) The LLM Developer must implement and maintain appropriate technical and organizational measures to ensure that all such Government Data is logically segregated from the Data of any non-Government customer or client, and is not commingled with Data of other customers or clients and provides adequate defense in depth through access controls, policy enforcement points, labeling, and/or encryption mechanisms and must perform continuous monitoring to protect against unauthorized access by external and internal threat actors, third parties, or disclosure resulting from human or machine error. Logical segregation does not require physical or dedicated instances within contractor-hosted or controlled systems, continuing compliance with the specified FedRAMP authorization level is deemed to satisfy these requirements by achieving equivalent security and separation.

(vii) Upon completion, termination or expiration of the contract or task/delivery order, unless otherwise directed in writing by the Contracting Officer, the LLM Developer must securely and permanently delete all such Government Data and any Custom Developments from the LLM and all its other systems and all copies, backups and derivatives thereof, and certify deletion to the Contracting Officer in writing.

(viii) *Custom Developments and Model Rights.* If there is a requirement for Custom Developments, the LLM Developer must:

- (A) Dedicate the Custom Developments, including any customized or enhanced models resulting from such Custom Developments, to the Government's exclusive use;
- (B) Treat such Custom Developments, custom models, and all associated Data as the Government's confidential information; and

(C) Not use, reproduce, or derive benefit from such Custom Developments or custom models for any other purpose, or for the benefit of any other party, without express written authorization from the Contracting Officer.

(ix) *Feedback*. The Government retains ownership of all feedback provided by the Government to the LLM Developer with respect to the LLM or Custom Developments, regardless of whether such feedback is generated by Government personnel, the LLM Developer, or through automated processes. If feedback includes Government Data and Government confidential information, that feedback may not be used for system improvement purposes or any other purposes (except solely in the performance of this contract).

(f) LLM Developer *Obligations for Compliance, Reporting, and Documentation*. The LLM Developer must:

(1) Disclose all LLMs used or made available under government contracts. Disclosures are due to the Contracting Officer or ordering Contracting Officer by the date specified in the contract or task/delivery order. If no date is specified, disclosures are due within 120 days after commencing work under the contract or task/delivery order.

(2) Maximize the use of LLMs that meet the following criteria:

(i) Controlling Entity & Jurisdiction: Each LLM is developed, managed, and operated by an entity that is incorporated in the United States (U.S.) and is subject to U.S. law and jurisdiction.

(ii) Protection Against Foreign Compulsion:

(A) Each LLM's performance, operations, or protections cannot be controlled by a foreign Government.

(B) No foreign Government or entity can compel disclosure of Government Data, or operational details that could compromise each LLM's integrity or security.

(C) Each LLM, and any LLM components performing core model, data storage or processing, output generation, or security functions, are prohibited from being developed, managed, or operated by entities subject to the direction, influence, or control of adversary foreign governments (see 15 CFR 791.4).

(iii) Component Flexibility & Risk Mitigation: Incidental foreign-developed components (e.g., open-source components, published research), ancillary Third-party services, or globally operated infrastructure dependencies are permissible, provided:

(A) They do not introduce security risks or foreign control that would violate criteria (f)(2)(i) or (f)(2)(ii).

(B) The systems storing or processing Government Data satisfy applicable Federal security requirements, including those for data residency and isolation.

(C) A risk-based approach is applied, focusing on objective criteria such as ownership, control, hosting, and security posture.

(3) Provide a means for the Government to implement human oversight, intervention, and traceability. If the LLM uses intermediary processing such as reasoning, retrieval, or agentic processes, the LLM must summarize intermediary steps from data input to data output, and make this information accessible through data output, audit trail, and as applicable the user interface, as part of the LLM Developer's products through the user interface for end-user products, or through documented API functionality when requested by the end user or API. The resulting explanation will include, as applicable:

(i) Summarized intermediate processing actions and decision points;

(ii) Model routing decisions with accompanying rationale; and

(iii) Data retrieval methods employed (e.g., Retrieval-Augmented Generation (RAG), web search, tool calls), including complete source attribution with direct links and relevant excerpts from materials used in response generation.

(4) Notify the Contracting Officer and any Government provided point of contacts as soon as possible but not longer than within 72 hours of the discovery of any incident (as defined by the Federal Information Security Modernization Act of 2014 in 44 U.S.C. § 3552(b)(2)) affecting any contractors, including Third-party entities, handling Government Data and provide daily status updates to all points of contact until resolved.

(i) Such notification must include, to the extent known at the time:

- (A) Nature and scope of the incident;
- (B) Data potentially affected;
- (C) Immediate remediation steps taken;
- (D) Timeline for full resolution; and
- (E) Measures to prevent recurrence.

(ii) Where FedRAMP incident communication and response procedures conflict with contractual requirements, the FedRAMP procedures take priority if the system is required to be FedRAMP Authorized.

(iii) The LLM Developer must preserve all relevant logs, forensic images, and incident artifacts for a minimum of 90 calendar days from a security incident involving Government Data to support follow-on investigation activity by law enforcement entities.

(iv) The LLM Developer must also complete the CISA incident reporting form (<https://myservices.cisa.gov/irf>).

(5) Provide, upon Government request, and under appropriate confidentiality protections, existing commercial documentation or disclosures sufficient to demonstrate compliance, including but not limited to:

(i) Verification of compliance with these terms and conditions and the contract;

(ii) List of entities involved in performance of a contract or task/delivery order, the entities' role(s), which requirements of these terms and conditions are applicable to each entity, and the entities' approach to addressing the requirements in these terms and conditions;

(iii) LLM decision-making processes, logic, and operational parameters;

(iv) LLM Developers, general model characteristics, intended use, limitations, and risk considerations to enable informed and responsible use by the Government. The contractor is not required to disclose proprietary source code, model weights, or trade secrets.

(v) System documentation consistent with NIST AI Risk Management Framework guidelines, Unbiased AI Principles, and LLM Transparency requirements such as system cards or equivalent documentation.

(vi) Transparency & Auditability: The LLM Developer must provide commercially available means for the Government to implement appropriate human oversight, intervention, and traceability for the contracted use case, and to understand the role of various components in generating responses, to the extent commercially available and technically feasible;

(vii) Privacy controls effectiveness and PII processing prohibition compliance;

(viii) Testing methodologies used to detect and mitigate noncompliance with the unbiased AI principles described in paragraph (j)(1);

(ix) Known biases (including commercial, political, or personal considerations, advertising, endorsements, or fraudulent/corrupt interests), limitations, truthfulness concerns, and performance metrics;

(x) Influence, direction, or control of an adversary foreign government (see 15 CFR 791.4);

(xi) FedRAMP authorization packages, continuous monitoring data, and assessment artifacts necessary to issue or maintain an authorization to operate, consistent with 44 U.S.C. § 3609(a)(8) and OMB M-24-15 and successor requirements; and

(xii) Any other information necessary for the Government to monitor and evaluate the LLM's performance, risks, and effectiveness and to complete an LLM Impact Assessment required by OMB M-25-21 and successor requirements.

(xiii)

(g) *Privacy and Confidentiality Protections.* To the extent the LLM Developer has available tools, they must provide tools to enable the Government to implement appropriate Government-configurable controls, including but not limited to automated detection mechanisms and clear user notifications to manage, the entry or persistence of PII within the LLM.

(h) *Data Portability and Interoperability.* The LLM Developer must:

(1) Provide and ensure that LLM services support the export of Government Data (including but not limited to: user-generated content, interaction history, uploaded content and media, and knowledge bases) in open or standard machine-readable formats, together with sufficient associated metadata and schema information necessary for the Government to retrieve, use, or migrate Government Data to another service.

(2) Provide and support documented APIs sufficient for Government integration and data export to the extent the service uses APIs.

(3) Not impose proprietary formats, technical restrictions, additional costs, or additional licensing conditions that materially impair the Government's ability to retrieve, use, or migrate Government Data to another service.

(4) Provide tooling or interfaces to facilitate migration of Government Data and Custom Developments in a secure manner.

(i) *Change Notification.*

(1) Service Deprecation. The LLM Developer will provide the Contracting Officer prior written notice at least thirty (30) calendar days before deprecating a generally available service made available under this contract. This obligation does not apply where a shorter period is required by law or reasonably necessary to address security, safety, or misuse.

(2) Advance Notice of Material Changes. The LLM Developer must maintain commercial practices to provide reasonable advance notice to the Contracting Officer prior to any planned material change affecting the services provided under this contract, including:

(i) Adding, replacing, or materially changing any LLMs, LLM's Developer(s), System Operator(s), System Integrator(s), or Service Provider(s);

(ii) Changes to the services handling Government Data, including discontinuation or material reduction of data protection controls applied to Government Data, or change in FedRAMP Authorization Status; or

(iii) Any modification, configuration, or training change to the LLM or services made available under this contract made to comply with any non-U.S. government statute, regulation, or policy.

(3) Model Version Changes. The LLM Developer must use reasonable efforts to provide the Government with concurrent access to any successor LLM, and associated documentation, for a minimum evaluation period of thirty (30) calendar days for major versions, and fifteen (15) calendar days for minor versions, prior to discontinuing or replacing any LLM in use under this contract.

(4) Safety and Performance Degradation. The LLM Developer must notify the Contracting Officer within seven (7) calendar days of identifying any change that materially increases output bias; decreases safety guardrails or behavioral constraints; or degrades performance or truthfulness of outputs. The notification must describe the change, its purpose, the evaluation approach used and any new limitations, trade-offs, or potential negative impacts identified.

(5) Emergency and Unplanned Changes. If the LLM Developer implements a change without providing sufficient advance notice, or if a change is necessitated by a security or service emergency, the LLM Developer must:

- (i) Notify the Contracting Officer as soon as practicable upon learning of the change; and
- (ii) Describe any remediation or rollback actions available.

(6) Notification: All notifications under paragraph (i) must include, to the extent known at the time of notification:

- (i) Description of change;
- (ii) Affected roles, services, systems, and Government Data;
- (iii) Any limitations, trade-offs, or negative impacts;
- (iv) Evaluation approach used to assess the change;
- (v) Any remediations or rollback actions; and
- (vi) Confirmation of applicable requirements of these terms and conditions have been flowed down appropriately.

(j) *Performance, Evaluation, and Remediation.*

(1) *Unbiased AI principles.* The LLM Developer will make best efforts to develop and monitor the LLM in accordance with the following unbiased AI principles:

- (i) The LLM must be truthful in responding to user prompts seeking factual information or analysis. The LLM must prioritize historical accuracy, scientific inquiry, and objectivity and must acknowledge uncertainty where reliable information is incomplete or contradictory.
- (ii) The LLM must be a neutral, nonpartisan tool that does not manipulate responses in favor of ideological dogmas. The LLM Developer must not intentionally introduce or embed partisan or ideological judgments into the LLM's Data Outputs through methods such as training data

selection, fine-tuning, Retrieval-Augmented Generation (RAG) references, system prompts, or other configuration methods.

(iii) The LLM Developer must implement continuous improvement processes to enhance detection and mitigation of performance, trustworthiness, bias, and/or systems generating illegal or prohibited content, including regular evaluation of system outputs (excluding Data Outputs) against verified factual sources.

(2) *Government Evaluation Rights and Remediation.*

(i) The Government reserves the right to conduct automated assessments of the LLM, as deployed and configured for government users, at any time using its own benchmarks. These evaluations may assess bias, truthfulness, safety, unsolicited ideological content, and other factors determined by the Government in order to facilitate evaluations.

(ii) The LLM Developer must provide tools and interfaces that enable the Government to run its benchmarks in an automated fashion to test the production LLM and identify any material gaps.

(iii) The Government may provide such results to the LLM Developer to support remediation efforts.

(iv) All benchmarks, test data, and methodologies developed or used by the Government for such assessments are considered Government Data. The Government is under no obligation to disclose or provide access to the underlying data, methodologies, or systems, with the exception of data or methodologies used as the basis for an adverse action.

(3) *Non-Compliance.*

(i) The Government retains the right to suspend use of the LLM until performance issues are satisfactorily addressed.