

PLATFORM SERVICES AGREEMENT

This Platform Services Agreement (together with any Order Forms and Service-Specific Terms, this “**Agreement**”) is by and between Sierra Technologies, Inc. (“**Sierra**”) and the customer identified on the applicable Order Form (“**Customer**”). This Agreement is effective as of the “Effective Date” listed on the initial Order Form that references this Agreement (the “**Effective Date**”). Sierra and Customer may be referred to collectively as the “**Parties**” or individually as a “**Party**.”

This Agreement is a framework agreement designed to govern Customer’s use of both the Paid POC Services and thereafter, the steady-state Platform Services, as more particularly described in the applicable Order Form.

1. PLATFORM SERVICES.

(a) Right to Use. Subject to Customer’s compliance with this Agreement, Sierra hereby grants to Customer a limited, non-exclusive, non-transferable (except under Section 13) right to access and use the Platform Services during the Term, solely to develop, test and deploy Customer Agents for the purpose of providing service and support to Customer’s end users and related internal business purposes, in accordance with the applicable Order Form.

(b) Use Restrictions. Unless expressly permitted in this Agreement, Customer will not and will not permit any other person or entity (including Authorized Users) to, directly or indirectly: (i) copy, modify or create derivative works of any portion of the Platform Services or Documentation; (ii) reverse engineer, decompile, disassemble or otherwise attempt to derive or extract the source code, models, algorithms or underlying systems of the Platform Services, including by model extraction, model stealing or prompt injection attacks, except as permitted by applicable law; (iii) sublicense, sell, resell, distribute, rent, lease, frame, mirror or otherwise make the Platform Services or Documentation available to any third party; (iv) use the Platform Services or Documentation in violation of applicable law, the AUP or any intellectual property or other rights of any third party; (v) access, search or scrape the Platform Services using any automated means (including spiders, crawlers, bots or other data-mining tools) other than features Sierra has expressly provided for that purpose; or (vi) use the Platform Services, Output or any other Sierra Confidential Information to develop or commercialize any competitive product, service or technology. Customer is responsible for all acts and omissions of its Authorized Users in connection with the Platform Services, including activities conducted through any access credentials issued by Sierra (e.g., API keys), and for their compliance with this Agreement.

(c) Third-Party Services. Certain features and functionalities within the Platform Services may allow Customer and its Authorized Users to interface or interact with, access and/or use compatible third-party services, products, technology and content that is provided or procured by Customer (collectively, “**Third-Party Services**”) through the Platform Services. Sierra does not provide any aspect of the Third-Party Services and is not responsible for any compatibility issues, errors or bugs in the Platform Services or Third-Party Services caused in whole or in part by the Third-Party Services or any update or upgrade to them. As between the Parties, Customer is responsible for maintaining the Third-Party Services and obtaining any associated licenses and consents necessary for Customer and its Authorized Users to use the Third-Party Services in connection with the Platform Services.

2. **PAID PROOF OF CONCEPT SERVICES.** Sierra will provide Paid POC Services to Customer as described in an Order Form for the period specified in that Order Form (the “**Paid POC Period**”) for the sole purpose of Customer evaluating the Platform Services. If the Parties agree to proceed with steady-state Platform Services following the Paid POC Period, they will execute a separate Order Form to govern the provision of such Platform Services.

3. **FEES.** Customer will pay Sierra or its authorized reseller as applicable the fees set forth in the applicable Order Form in accordance with the GSA Schedule Pricelist (“**Fees**”) in accordance with the payment terms set forth in that Order Form. Except as otherwise provided in the applicable Order Form or agreed to by the Parties in writing, Sierra or its authorized reseller as applicable will issue invoices to Customer during the Term, and Customer will pay all amounts set forth on any such invoice no later than thirty (30) days after the date of such invoice. If Customer in good faith disputes any portion of an invoice, Customer will notify Sierra in writing within the same period, providing a reasonably detailed explanation of the disputed amount and the grounds for the dispute. The Parties will cooperate in good faith to resolve any disputed amounts. The undisputed portion of any invoice remains due and payable in accordance with this Section 3. Fees for Platform Services delivered or made available to Customer are earned upon delivery and are not subject to refund. Neither Party may set off, discount or otherwise reduce or refuse to pay any amount due to the other Party under this Agreement, except that, if the Parties execute an Order Form for steady-state Platform Services, Customer will receive a one-time credit of the Fees paid for the Paid POC Services against the Fees payable under that Order Form. If Customer fails to pay any undisputed amount when due, then without limiting Sierra's rights or remedies: (i) reserved; and (ii) interest will accrue on the outstanding amount at the interest rate established by the Secretary of the Treasury as provided in [41 U.S.C. 7109](#), which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. If Customer is required to deduct or withhold any taxes from the amounts payable to Sierra under this Agreement, Customer will make

gross up payments, so that Sierra receives the amounts due to it under this Agreement in full, as if there were no withholding or deduction.

4. OWNERSHIP AND USE.

(a) Rights Reserved. Sierra reserves and, as between the Parties will solely own, the Sierra IP and all rights, title and interest in and to the Sierra IP. If any rights, title or interest in or to any Sierra IP vests in Customer, Customer hereby assigns to Sierra such rights, title or interest.

(b) Customer Materials. The Customer Materials will be deemed Confidential Information of Customer and, as between the Parties, Customer owns and retains all rights, title and interest in and to all Customer Materials. If any rights, title or interest in or to any Customer Materials vests in Sierra, Sierra hereby assigns to Customer such rights, title or interest.

(c) Input and Output. Customer Agents may generate automated responses, actions or suggestions (collectively, “**Output**”) in response to: (i) a message, chat, ticket or other interaction submitted by an end user to a Customer Agent; and (ii) Customer Materials uploaded by Customer to inform a Customer Agent’s responses to end users ((i) and (ii) collectively, “**Input**”). Input and Output will be deemed Confidential Information of Customer. As between the Parties, to the extent permitted by applicable law and subject to Section 4(a), Customer owns all Input and Output. If any rights, title or interest in or to any Input or Output vests in Sierra, Sierra hereby assigns to Customer such rights, title or interest.

(d) No Implied Rights. Except as expressly granted in this Agreement, no rights or licenses (whether by implication, estoppel or otherwise) are granted to either Party or any Affiliate in or to the Sierra IP, the Customer Materials, Input or Output.

(e) Use of Customer Materials, Input and Output. Sierra may use and modify the Customer Materials, Input and Output to provide and improve the Platform Services for the sole benefit of Customer during the Term, to enforce the terms of this Agreement and to comply with applicable law. Sierra may also use and modify Customer Materials, Input and Output that have been deidentified of personally identifiable information to maintain, develop and improve its products and services.

(f) Usage Data. Sierra may collect, derive and use usage data, insights, metadata and other telemetry data and information based on Customer Materials, Input, Output and Customer’s and its Authorized Users’ use of the Platform Services (“**Usage Data**”) on a deidentified basis in order to provide and improve its products and services. Sierra will not share any Usage Data with a third party unless it has been aggregated and anonymized such that Customer and its Authorized Users cannot be identified.

(g) DPA. The terms of the attached Data Processing Addendum (“**DPA**”) govern Sierra’s processing of Personal Data contained within Customer Materials.

(h) Feedback. From time-to-time Customer may provide Sierra with suggestions, comments or feedback with regard to the Platform Services (collectively, “**Feedback**”), which Sierra may use and exploit in connection with Sierra’s business purposes, including the operation, maintenance and improvement of Sierra’s products and services. Sierra 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.

5. REPRESENTATIONS AND WARRANTIES.

(a) General. Each Party represents and warrants to the other Party that: (i) it has full power and authority to enter into this Agreement; (ii) the execution, delivery and performance of this Agreement by it have been duly authorized by all necessary actions and do not violate its organizational documents; and (iii) it will comply with the laws applicable to that Party’s exercise of its rights and performance of its obligations under this Agreement. Customer acknowledges that: (a) Sierra is not responsible for determining whether Customer’s use of the Platform Services complies with any laws that apply to Customer; and (b) Customer may be subject to laws relating to the deployment and use of the Platform Services, and that Customer shall be responsible for their own compliance obligations. Each Party will provide information reasonably requested by the other Party to assist the other Party in its compliance obligations.

(b) Customer Representations. Customer represents and warrants that: (i) Sierra’s use of the Customer Materials in accordance with this Agreement will not infringe or violate any intellectual property or other rights of any third party; and (ii) it has all rights and permissions required to submit the Customer Materials and Input to the Platform Services for use in accordance with this Agreement.

(c) Sierra Representations. Sierra represents and warrants that: (i) Customer’s use of the Platform Services in accordance with this Agreement will not infringe or violate any intellectual property or other rights of any third party; (ii) it has all rights and permissions required to provide the Platform Services in accordance with this Agreement; and (iii) the Platform Services will operate

during the Term substantially as described in the applicable Documentation.

(d) Disclaimers.

(i) AS IS. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, THE PLATFORM SERVICES AND OTHER SIERRA IP ARE PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, SIERRA DISCLAIMS ALL WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND TITLE.

(ii) Nature of the Platform Services. Due to the non-deterministic nature of large language models, Customer acknowledges that Output may be (a) similar to the output generated for Sierra or for a third party; and (b) inaccurate, incomplete or otherwise inappropriate for a given use case. The accuracy, quality and compliance with applicable law of any Output and actions taken by Customer Agents are dependent upon and commensurate with that of the Input provided and Customer’s compliance with this Agreement. Customer further acknowledges that the software code for Customer Agents developed by or on behalf of Customer under this Agreement may be similar to software code developed by or for other Sierra customers through use of the Platform Services, subject always to the confidentiality obligations set forth in Section 10.

(iii) Customer Responsibility. As between the Parties, Customer is responsible for: (i) evaluating the content, nature, tone and accuracy of any Output as appropriate for the applicable use case before relying or acting on it; (ii) ensuring that Customer’s use of the Platform Services and Customer Agents complies with all laws and regulations applicable to Customer or its industry; and (iii) the development, use, deployment or operation of any Customer Agent to the extent developed by or on behalf of Customer.

6. SUPPORT AND SERVICE LEVELS. Except as otherwise set forth in an Order Form, Sierra will comply with the Support Terms.

7. TERM. The term of this Agreement begins on the Effective Date and continues until the end of the Paid POC Period, except that if the Parties execute an Order Form for steady-state Platform Services, the term of this Agreement will continue for the initial term specified in such Order Form (together, the “**Initial Term**”). Unless the applicable Order Form specifies otherwise, the Initial Term may be renewed for successive periods of twelve (12) months (each, a “**Renewal Term**”) by executing a written order. The Initial Term, together with any Renewal Term(s), are collectively the “**Term**”.

8. TERMINATION. When the End User is an instrumentality of the U.S., 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, Sierra 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

9. EFFECT OF TERMINATION.

(a) Effect. Upon expiration or termination of an Order Form or this Agreement: (i) each Party will cease use of and will promptly return or destroy any Confidential Information of the other Party in its possession or control that is specific to such Order Form or to this Agreement (as applicable), except (A) as required for any surviving rights or obligations under such Order Form or this Agreement (as applicable); and (B) for any archived electronic backups, which will be stored in accordance with the applicable Party’s backup retention policies and will remain subject to the confidentiality obligations set forth in Section 10; (ii) Customer’s and its Authorized Users’ right to access and use the Platform Services under such Order Form or this Agreement (as applicable) will immediately terminate; and (iii) all Fees owed by Customer to Sierra under such Order Form or this Agreement (as applicable) will be immediately due. Upon expiration or termination of an Order Form (other than termination of the entire Agreement under Section 8), each other Order Form that is then-in effect will remain in effect in accordance with its terms.

(b) Survival. The rights and obligations of Sierra and Customer contained in Sections 3, 4, 9, 10, 11, 12, 13 and 14, will survive any expiration or termination of this Agreement and any Order Form(s).

10. CONFIDENTIALITY.

(a) Confidentiality. As used in this Agreement, “**Confidential Information**” means any information that one Party (the “**Disclosing Party**”) provides to the other Party (the “**Receiving Party**”) in connection with this Agreement, whether orally or in writing, that is designated as confidential or that reasonably should be considered to be confidential given the nature of the information and/or

the circumstances of disclosure. For clarity, the Sierra IP will be deemed Confidential Information of Sierra. The Receiving Party will only use the Disclosing Party's Confidential Information to exercise the Receiving Party's rights and fulfill its obligations under this Agreement, and will use the same degree of care (but not less than reasonable care) that it uses to protect its own Confidential Information. The Receiving Party will: (i) not use or disclose any Confidential Information of the Disclosing Party except as expressly permitted in this Agreement; and (ii) limit access to Confidential Information to those of its and its Affiliates' employees, contractors, agents and advisors who have a bona fide need to know such Confidential Information to perform under this Agreement and who are bound by written agreements with use and nondisclosure restrictions at least as protective of Confidential Information as those set forth in this Agreement. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent such disclosure may be required by the order or requirement of a court, administrative agency or other governmental body, subject to, but only to the extent permitted by applicable law, the Receiving Party providing the Disclosing Party with reasonable written notice to allow the Disclosing Party to seek a protective order or otherwise contest the disclosure, in each case, at the Disclosing Party's own cost. The terms of this Agreement will constitute Confidential Information of each Party but may be disclosed on a confidential basis to a Party's advisors, attorneys and actual or bona fide potential acquirers, investors or other sources of funding (and their respective advisors and attorneys) for due diligence purposes.

(b) Exclusions. Confidential Information will not include any information that: (i) is or becomes generally known to the public through no fault or breach of this Agreement by the Receiving Party; (ii) is rightfully known by the Receiving Party at the time of disclosure without an obligation of confidentiality; (iii) is independently developed by the Receiving Party without access to or use of any Confidential Information of the Disclosing Party as evidenced in writing; (iv) is rightfully obtained by the Receiving Party from a third party without restriction on use or disclosure; or (v) is Personal Data (which, to the extent applicable, will be subject to the DPA). Sierra 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. To the extent permitted by applicable law and the agency's FOIA regulations, Customer will notify Sierra of any FOIA request that encompasses Sierra's confidential or proprietary information.

11. LIMITATION OF LIABILITY.

(a) Exclusion of Damages. TO THE EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF INCOME, DATA, GOODWILL, PROFITS, REVENUE OR BUSINESS INTERRUPTION, OR THE COST OF COVER OR SUBSTITUTE SERVICES, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, WHETHER OR NOT SUCH PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. 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.

(b) Total Liability. TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY'S TOTAL CUMULATIVE LIABILITY TO THE OTHER EXCEED THE FEES PAID BY CUSTOMER TO SIERRA IN THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY (THE "**GENERAL CAP**"). NOTWITHSTANDING THE FOREGOING, IN NO EVENT WILL EITHER PARTY'S TOTAL CUMULATIVE LIABILITY TO THE OTHER IN CONNECTION WITH A BREACH OF THE DPA THAT RESULTS IN A SECURITY INCIDENT (AS DEFINED IN THE DPA) EXCEED TWO (2) TIMES THE FEES PAID BY CUSTOMER TO SIERRA IN THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY (THE "**ENHANCED CAP**"). THE PARTIES ACKNOWLEDGE THAT THE LIABILITY CAPS ARE INTENDED TO OPERATE AS A SINGLE AGGREGATE LIMIT AND THE ENHANCED CAP IS INCLUSIVE OF, AND NOT IN ADDITION TO, THE GENERAL CAP. THE EXISTENCE OF MORE THAN ONE CLAIM WILL NOT ENLARGE THESE LIMITS.

(c) Exceptions. THE FOREGOING EXCLUSIONS AND LIMITS IN SECTION 11(a) AND SECTION 11(b) DO NOT APPLY TO LIABILITY OR OBLIGATIONS ARISING UNDER SECTION 1(b) (USE RESTRICTIONS), CUSTOMER'S PAYMENT OBLIGATIONS, INFRINGEMENT OR MISAPPROPRIATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS AND EACH PARTY'S INDEMNITY OBLIGATIONS UNDER SECTION 12(a) AND SECTION 12(c).

(d) General. THE LIMITATIONS AND EXCLUSIONS IN THIS SECTION 11 WILL APPLY WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE.

12. INDEMNIFICATION.

(a) Indemnification by Sierra. Subject to Section 12(b), Sierra will have the right to intervene to defend Customer from and against any claims, demands, proceedings, investigations or suits brought by a third party alleging that the Platform Services provided by Sierra infringes or misappropriates such third party's intellectual property rights (each, a "**Claim Against Customer**") and indemnify Customer for any finally awarded damages or settlement amount approved by Sierra in writing to the extent arising from a Claim Against Customer, and any reasonable, documented and out-of-pocket attorneys' fees of Customer incurred in connection with such Claim Against Customer. If Sierra reasonably believes the Platform Services (or any component of the Platform Services) could infringe any third party's intellectual property rights, Sierra may, at its sole option and expense, use commercially reasonable efforts to: (i) modify or replace the Platform Services, or any component or part of the Platform Services, to make it non-infringing; or (ii) procure the right for Customer to continue to access and use the Platform Services. If Sierra determines that neither alternative is commercially practicable, Sierra may terminate this Agreement, in its entirety or with respect to the affected component, by providing written notice to Customer. In the event of any such termination, Sierra will refund to Customer a pro-rata portion of the Fees that have been paid but unused for the unexpired portion of the then-current Term. The rights and remedies set forth in this Section 12 will constitute Customer's sole and exclusive remedy for any infringement or misappropriation of intellectual property rights in connection with the Platform Services. 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.

(b) Exclusions. Sierra's obligations under Section 12(a) will not apply to the extent that the underlying Claim Against Customer arises from or as a result of: (i) Customer's breach of this Agreement, negligence, willful misconduct or fraud; (ii) any Customer Materials, Input or Output; (iii) Customer's failure to use any enhancements, modifications or updates to the Platform Services that have been provided by Sierra; (iv) modifications to or configuration of the Platform Services by anyone other than Sierra, including portions of Customer Agents to the extent developed by or on behalf of Customer; or (v) combinations of a Customer Agent or the Platform Services with Third-Party Services or any other software, data or materials not provided by Sierra.

(c) Procedure. Each Party's obligations under this Section 12 are contingent upon: (i) the Party seeking defense and indemnity (the "**Indemnified Party**") providing the other Party (the "**Indemnifying Party**") with prompt written notice of the Claim Against Customer or Claim Against Sierra, as applicable (each, a "**Claim**") (but in any event notice in sufficient time for the Indemnifying Party to respond without prejudice); (ii) the Indemnifying Party having the exclusive right to defend or settle such Claim; and (iii) the Indemnified Party providing all reasonably necessary cooperation to the Indemnifying Party, at the Indemnifying Party's expense, in the defense and settlement of such Claim. The Indemnifying Party will have the sole right to conduct the defense of any Claim for which the Indemnifying Party is responsible under this Agreement (provided that the Indemnifying Party will not settle any Claim without the Indemnified Party's prior written approval, not to be unreasonably withheld, unless the settlement is for a monetary amount, unconditionally releases the Indemnified Party from all liability without prejudice, does not require any admission by the Indemnified Party and does not place restrictions upon the Indemnified Party's business, products or services). The Indemnified Party may participate in the defense of any Claim at its own expense, subject to the Indemnifying Party's retention of overall control over the defense and settlement of the Claim.

13. MISCELLANEOUS. Neither Party may assign, transfer or sublicense this Agreement, by operation of law or otherwise, without the other Party's prior written consent, except to a successor entity in the event of a merger, consolidation or sale of all or substantially all of the assets of such Party, and any attempt by either Party to do so, without such consent, will be void. Subject to the foregoing, this Agreement is binding upon and will inure to the benefit of each of the Parties and their respective successors and permitted assigns. The Platform 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 Platform Services and Documentation are: (a) provided to Customer and Authorized Users for use by Customer or on its behalf and (b) subject to this Agreement and with only those rights as are granted to all other customers and end users of Sierra, except to the limited extent prohibited by applicable law. Each Party agrees to comply fully with all relevant export control and sanctions laws and regulations of the United States ("**Export Laws**") to ensure that neither the Platform Services, software, any Customer Materials, nor any technical data related to any of them is: (i) used, exported or re-exported directly or indirectly in violation of Export Laws; or (ii) used for any end use prohibited by the Export Laws. Customer will complete all undertakings required by Export Laws, including obtaining any necessary export license or other governmental approval. Subject to the DPA, Sierra may use subcontractors and other third-party providers ("**Subcontractors**") in connection with the performance of its own obligations under this Agreement as it deems appropriate; provided that Sierra remains responsible for the performance of each such Subcontractor. Neither Party will be responsible for any failure or delay in the performance of its obligations under this Agreement (except for any payment obligations) due to causes beyond its reasonable control. If any provision of this Agreement is held invalid, illegal or unenforceable, that provision will be enforced to the maximum extent permitted by applicable law, given the fundamental intentions of the Parties, and the remaining provisions of this Agreement will remain in full force and effect. This Agreement, including its exhibits and any Order Form(s), is the complete and exclusive agreement between the Parties with respect to its subject matter and supersedes all prior or contemporaneous agreements, communications and understandings, both written and oral, with respect to its subject matter. Each Party acknowledges that, in entering into this Agreement, it has not relied on any statement, representation, warranty or assurance other than those expressly set out in this Agreement, except that nothing in this Agreement excludes or limits liability for fraud or fraudulent misrepresentation. This Agreement

may be amended or modified only by a written document executed by duly authorized representatives of the Parties. If there is any conflict, the following order of precedence applies: (1) the applicable Service-Specific Terms with respect to the relevant service; (2) the DPA with respect to the Processing of Personal Data; (3) the terms of this Agreement; (4) the applicable Order Form; (5) the Support Terms; (6) the AUP; and (7) the Documentation. Notwithstanding the foregoing order of precedence, to the extent that an Order Form explicitly states that it intends to modify the terms of any other document, then that Order Form supersedes the term that it seeks to amend. Nothing in this Agreement creates a partnership, joint venture or agency relationship between the Parties. Neither Party will have the power to bind the other or to incur obligations on the other's behalf without such other Party's prior written consent. Nothing in this Agreement creates any rights, benefits or obligations in any person other than the Parties. Except as expressly set forth in this Agreement, the exercise by either Party of any remedy under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise. No failure or delay by either Party to enforce any provision will constitute a waiver, and no waiver will be effective unless in writing and signed by the Party granting it. Any terms contained or referenced in any purchase order, procurement portal, invoice or other ordering document of Customer that are inconsistent with or additional to this Agreement are hereby rejected by the Parties and will be deemed null and of no force and effect. All notices required to be sent under this Agreement will be in writing (email being sufficient) and will be deemed to have been given when mailed by certified mail, overnight express or sent by email, with receipt confirmed. Email notices to Sierra should be sent to legal@sierra.ai. This Agreement will be governed by and construed in accordance with the laws of the State of California without giving effect to any principles of conflict of laws that would lead to the application of the laws of another jurisdiction. The Parties expressly agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply. Any legal action or proceeding arising under this Agreement will be brought exclusively in the federal or state courts located in the Northern District of California, and the Parties irrevocably consent to the personal jurisdiction and venue of those courts. This Agreement may be signed in counterparts, and electronic signatures will have the same weight and effect as originals.

14. DEFINITIONS.

"Affiliate" means any entity that directly or indirectly controls, is controlled by or is under common control with a party, where "control" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"AUP" means Sierra's [Acceptable Use Policy](#), which forms part of this Agreement.

"Authorized Users" means: (i) in the case of elements of the Platform Services other than Customer Agents, Customer's employees and contractors authorized to access the Platform Services; and (ii) in the case of Customer Agents, Customer's end users, employees and contractors that Customer permits to access the Customer Agents.

"Customer Agent" means an AI-enabled system that is developed by or on behalf of Customer under this Agreement and designed to function as part of and interoperate with the Platform Services.

"Customer Materials" means all information, data, conversations, content or other materials, in any form or medium, that are provided, communicated or otherwise uploaded by or on behalf of Customer or its Authorized Users through the Platform Services or to Sierra in connection with Customer's or its Authorized Users' use of the Platform Services, excluding any Sierra IP.

"Documentation" means the operator, user and technical manuals, readme files and other documentation provided by Sierra within the Platform Services.

"Order Form" means a mutually executed order form or other mutually agreed upon ordering document, in each case, that references and is made subject to this Agreement.

"Paid POC Services" means Platform Services made available by Sierra to Customer for a limited proof of concept period solely for the purpose of Customer evaluating the Platform Services.

"Personal Data" has the meaning set forth in the DPA.

"Platform Services" means Sierra's proprietary platform for delivering customer service, including: (i) Customer Agents; (ii) the software development kit and related libraries and materials made available as Agent SDK ("**Agent SDK**"); (iii) the functionality provided by Sierra to enable Customer to develop, configure and deploy Customer Agents ("**Agent Studio**"); and (iv) any other features, functionality, modules, add-ons or other technology identified in the applicable Order Form as Platform Services, together with the underlying technology, models and infrastructure used to provide or deliver any of the foregoing.

"Service-Specific Terms" means the additional terms that apply to a particular part of the Platform Services as (i) set out in or attached

to the applicable Order Form; or (ii) agreed to in a separate written instrument signed by both Parties.

“Sierra IP” means (i) the Platform Services and Documentation, together with the underlying intellectual property used to provide or resulting from the provision of the Platform Services or Documentation; (ii) all improvements, configurations, modifications or enhancements to, or derivative works of, the foregoing, regardless of inventorship or authorship; and (iii) all intellectual property rights in and to any of the foregoing.

Last Updated: July 8, 2026

DATA PROCESSING ADDENDUM

This Data Processing Addendum (including its Exhibits) (“**Addendum**” or “**DPA**”) forms part of and is subject to the terms and conditions of the Platform Services Agreement between the Customer listed on the Order Form (“**Customer**”) and Sierra Technologies, Inc. (“**Sierra**”) (the “**Agreement**”). Sierra and Customer may be referred to collectively as the “**Parties**” or individually as a “**Party**.”

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State solely to the extent that is inconsistent with the Federal law of the United States; all other provisions of this DPA remain in full force and effect.

1. SUBJECT MATTER, SCOPE, AND DURATION.

(a) Subject Matter. This Addendum reflects the Parties’ commitment to abide by Data Protection Laws concerning the Processing of Customer Personal Data in connection with the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum will control.

(b) Roles. The Parties agree that with respect to the Processing of Customer Personal Data under this Addendum, Sierra will act as Processor or subprocessor to Customer, who can act either as Controller or Processor of Customer Personal Data. For the avoidance of doubt, to the extent Processing of Customer Personal Data is subject to the CCPA, the Parties agree that Customer is the “Business” and Sierra is the “Service Provider” (as those terms are defined by the CCPA).

(c) Duration and Survival. This Addendum will become legally binding upon the effective date of the Agreement or upon the date that the Parties sign this Addendum if it is completed after the effective date of the Agreement. Sierra will Process Customer Personal Data until the relationship terminates as specified in the Agreement or as otherwise specified in this Addendum.

2. DEFINITIONS.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.

“**Customer Personal Data**” means Personal Data within the Customer Materials Processed by Sierra in its provision of the Platform Services.

“**Data Privacy Framework**” means the EU-U.S. Data Privacy Framework (and the UK Extension to the EU-U.S. Data Privacy Framework) and/or the Swiss-US Data Privacy Framework self-certification program operated by the U.S. Department of Commerce.

“**Data Privacy Principles**” means the Data Privacy Framework principles (as supplemented by the supplemental principles).

“**Data Protection Laws**” means the data privacy, data protection, and cybersecurity laws, rules and regulations applicable to the Processing of Customer Personal Data under the Agreement. “Data Protection Laws” may include, but are not limited to, the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) (“**CCPA**”) and other applicable U.S. federal and state privacy laws; the EU General Data Protection Regulation 2016/679 (“**GDPR**”) and its respective national implementing legislations; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time).

“**Personal Data**” means any information defined as “personally identifiable information,” “personal data,” “sensitive personal data,” “special categories of personal data,” “personal information” or any other analogous term under Data Protection Laws.

“**Platform Services**” has the meaning set forth in the Agreement.

“**Process**” or “**Processing**” means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction,

erasure, or destruction.

“**Processor**” means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “Service Provider” as that term is defined by the CCPA.

“**Security Incident(s)**” means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data attributable to Sierra.

“**Subprocessor(s)**” means Processors authorized by Sierra to Process Customer Personal Data.

3. PROCESSING TERMS FOR CUSTOMER PERSONAL DATA.

(a) Documented Instructions. Sierra will Process Customer Personal Data to provide the Platform Services in accordance with the Agreement, this Addendum, any applicable Statement of Work, and any instructions agreed upon by the Parties. Sierra will, unless legally prohibited from doing so, inform Customer in writing if (i) it reasonably believes there is a conflict between Customer’s instructions and applicable law or (ii) Sierra otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer’s instructions.

(b) Authorization to Use Subprocessors. Customer hereby authorizes Sierra to engage Subprocessors. Customer acknowledges that Subprocessors may further engage vendors.

(c) Sierra and Subprocessor Compliance. Sierra will: (i) enter into a written agreement with Subprocessors regarding such Subprocessors’ Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements that protect Customer Personal Data that are substantially similar to this Addendum; and (ii) remain responsible to Customer for Sierra’s Subprocessors’ failure to perform their obligations with respect to the Processing of Customer Personal Data.

(d) List of Sierra’s Subprocessors. A list of Sierra’s current Subprocessors is made available through the Sierra Trust Center, available at <https://trust.sierra.ai/> (the “**Subprocessor List**”). The Subprocessor List identifies the Subprocessors, their country or region locations, and their processing activities as they pertain to Customer Personal Data. Customer hereby consents to the Subprocessors on the Subprocessor List. Sierra will provide notification of a new Subprocessor by updating the Subprocessor List through the Trust Center and, for any Customer contact that subscribes or is otherwise designated to receive such notices, by email.

(e) Right to Object to New Subprocessors. Where required by Data Protection Laws, Customer may object to Sierra’s use of a new Subprocessor by notifying Sierra promptly in writing within ten (10) days after Sierra provides notice of the new Subprocessor in accordance with Section 3(d). If Customer has legitimate objections to the appointment of any new Subprocessor, the Parties will work together in good faith to resolve the grounds for the objection.

(f) Confidentiality. Any person authorized to Process Customer Personal Data must be subject to a duty of confidentiality, contractually agree to maintain the confidentiality of such information, or be under an appropriate statutory obligation of confidentiality.

(g) Personal Data Inquiries and Requests. Where required by Data Protection Laws, Sierra agrees to provide reasonable assistance to Customer, taking into account the nature of the Processing and the information available to Sierra, to help Customer respond to requests from individuals exercising rights in Customer Personal Data. If Sierra receives such a request directly, Sierra will, to the extent legally permitted, promptly forward the request to Customer and will not respond to the request except on Customer’s documented instructions or as required by applicable law.

(h) Data Protection Assessment, Data Protection Impact Assessment, and Prior Consultation. Where required by Data Protection Laws, Sierra agrees to provide reasonable assistance and information to Customer where, in Customer’s reasonable judgment, the type of Processing performed by Sierra requires a data protection assessment, data protection impact assessment, and/or prior consultation with the relevant data protection authorities. Customer will reimburse Sierra for reasonable, pre-approved out-of-pocket costs Sierra incurs in performing extraordinary assistance under this Section, unless the assistance is required due to Sierra’s breach of this Addendum.

(i) Demonstrable Compliance. Sierra will make available through the Sierra Trust Center, and upon Customer’s reasonable request, information reasonably necessary to demonstrate Sierra’s compliance with this Addendum, including applicable third-party certifications, audit reports, security documentation, and other materials. To the extent such information is not reasonably sufficient for Customer to meet its obligations under Data Protection Laws, Sierra will provide additional reasonable information, subject

to the confidentiality obligations in the Agreement and reasonable restrictions designed to protect Sierra systems, confidential information, and other customers' data.

(j) California Specific Terms. To the extent that Sierra's Processing of Customer Personal Data is subject to the CCPA, this Section will also apply. Customer discloses or otherwise makes available Customer Personal Data to Sierra for the limited and specific purpose of Sierra providing the Platform Services to Customer in accordance with the Agreement and this Addendum. Sierra will: (i) comply with its applicable obligations under the CCPA; (ii) provide the same level of protection as required under the CCPA; (iii) notify Customer if it can no longer meet its obligations under the CCPA; (iv) not "sell" or "share" (as such terms are defined by the CCPA) Customer Personal Data; (v) not retain, use, or disclose Customer Personal Data for any purpose (including any commercial purpose) other than to provide the Platform Services under the Agreement or as otherwise permitted under the CCPA; (vi) not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Sierra; and (vii) unless otherwise permitted by the CCPA, not combine Customer Personal Data with Personal Data that Sierra: (a) receives from, or on behalf of, another person; or (b) collects from its own, independent consumer interaction. Customer may: (1) take reasonable and appropriate steps agreed upon by the Parties to help ensure that Sierra Processes Customer Personal Data in a manner consistent with Customer's CCPA obligations; and (2) upon notice, take reasonable and appropriate steps agreed upon by the Parties to stop and remediate unauthorized Processing of Customer Personal Data by Sierra.

(k) Security. Sierra will implement and maintain reasonable administrative, technical, organizational and physical safeguards (collectively, the "Security Measures") designed to protect Customer Personal Data including the safeguards as described in Sierra's Security Exhibit, a current version attached hereto as Exhibit B. Notwithstanding any provision to the contrary, Sierra may modify the Security Measures in its sole discretion provided that such modification does not result in a material degradation to the protection of Customer Personal Data described in the Security Measures.

4. SECURITY INCIDENTS. Upon becoming aware of a Security Incident, Sierra agrees to provide written notice without undue delay and within the time frame required under Data Protection Laws to Customer's Designated POC. Where possible, such notice will include available details required under Data Protection Laws for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident. Where it is not possible to provide all relevant information at the same time, Sierra may provide the information in phases without undue further delay.

5. CROSS-BORDER TRANSFERS OF CUSTOMER PERSONAL DATA.

(a) Order of Precedence. In the event the Platform Services are covered by more than one transfer mechanism, the transfer of Customer Personal Data will be subject to a single transfer mechanism. These transfer mechanisms will apply in the following order of precedence: (i) the Data Privacy Framework (Section 5(b)); (ii) the EU Standard Contractual Clauses (Section 5(d)); or (iii) if none of the foregoing apply, any other data transfer mechanism permitted under Data Protection Laws.

(b) Data Privacy Framework. To the extent Sierra processes any Customer Personal Data via the Platform Services originating from the European Economic Area ("EEA"), Switzerland, or the United Kingdom, Sierra represents that Sierra Technologies, Inc. is self-certified under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, and complies with the Data Privacy Principles where processing any such Customer Personal Data. To the extent that Customer is (i) located in the United States of America and is self-certified under the Data Privacy Framework or (ii) located in the EEA, Switzerland, or the United Kingdom, Sierra further agrees (x) to provide at least the same level of protection to any Customer Personal Data as required by the Data Privacy Principles; (y) to notify Customer in writing, without undue delay, if its self-certification to the Data Privacy Framework is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative transfer mechanism will apply in accordance with the order of precedence in Section 5(a) (Order of Precedence)); and (z) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of Customer Personal Data.

(c) Cross-Border Transfers of Customer Personal Data. Customer hereby authorizes Sierra and its Subprocessors to transfer Customer Personal Data across international borders, including from the EEA, Switzerland, and/or the United Kingdom to the United States, in accordance with Section 5(a).

(d) EEA, Swiss, and UK Standard Contractual Clauses. If Customer Personal Data originating in the EEA, Switzerland, and/or the United Kingdom is transferred by Customer to Sierra in a country that has not been found to provide an adequate level of

protection under applicable Data Protection Laws, the Parties agree that the transfer will be governed by Module Two's (to the extent Customer is a Controller of Customer Personal Data) or by Module Three's (to the extent Customer is a Processor of Customer Personal Data) obligations in the [Annex to the Commission Implementing Decision \(EU\) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation \(EU\) 2016/679 of the European Parliament and of the Council \("Standard Contractual Clauses"\)](#) as supplemented by [Exhibit A](#) attached hereto, the terms of which are incorporated herein by reference. Each Party's signature to the Order Form entered into by the Parties pursuant to the Agreement will be considered a signature to this Addendum and the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder. References in this Addendum to the Standard Contractual Clauses, UK Addendum, or related linked transfer terms include any successor or updated version of such terms made available at the applicable link or successor URL, to the extent such successor or updated version is required or permitted under Data Protection Laws.

(e) Additional Jurisdiction-Specific Transfer Terms. Sierra will ensure that the same protections and obligations as set forth in the Standard Contractual Clauses apply to transfers from jurisdictions where legally adequate transfer mechanisms are required by applicable Data Protection Laws, and such terms will be interpreted by the Parties in good faith to apply to the maximum extent to such transfers. Where the measures and terms of the Standard Contractual Clauses do not adequately satisfy the requirements of such additional jurisdictions, the Parties may amend this DPA with jurisdiction-specific terms, as reasonably agreed and as practicable given Sierra's Platform Services and Sierra's related technical and organizational measures.

6. THIRD PARTY CERTIFICATIONS AND AUDIT RESULTS. Sierra has attained the third-party certifications and audit results set forth in the Sierra Trust Center. Upon Customer's reasonable request, and subject to the confidentiality obligations set forth in the Agreement, Sierra will make available to Customer a copy of Sierra's then most recent third-party certifications or audit results, as applicable.

7. CUSTOMER PERSONAL DATA DELETION. At the expiry or termination of the Agreement, Sierra will delete Customer Personal Data in accordance with its standard deletion process, excluding any back-up or archival copies which will be isolated, protected, and deleted in accordance with Sierra's data retention schedule, except where Sierra is required to retain copies under applicable laws. Upon Customer's request before deletion, Sierra will make Customer Personal Data available for export in a reasonably readable electronic format where technically feasible. Upon Customer's written request, Sierra will provide written confirmation of deletion after completion of its standard deletion process.

8. CUSTOMER COMPLIANCE. Customer represents and warrants that it has complied and will comply with all applicable Data Protection Laws in the performance of its obligations and exercise of its rights under the Agreement, including the provision of any applicable notices to Customer's end users and obtaining all necessary rights and consents for Sierra to Process all Customer Materials provided by or on behalf of the Customer. Customer further represents and warrants that it will include in each Customer Agent a legally adequate notice prior to each end user interaction containing: (i) a notice of recording of interactions by both Customer and its service provider; (ii) a link to Customer's privacy policy; and (iii) a reference to the use of an AI powered virtual agent.

9. PROCESSING DETAILS.

- (a) Subject Matter. The subject matter of the Processing is the Platform Services pursuant to the Agreement.
- (b) Duration. The Processing will continue until the expiration or termination of the Agreement.
- (c) Categories of Data Subjects. Data subjects whose Customer Personal Data will be Processed pursuant to the Agreement.
- (d) Nature and Purpose of the Processing. The purpose of the Processing of Customer Personal Data by Sierra is the performance of the Platform Services.
- (e) Types of Customer Personal Data. Customer Personal Data that is Processed pursuant to the Agreement.

10. CONTACT INFORMATION. Customer and Sierra agree to designate a point of contact for urgent privacy and security issues (a "Designated POC"). The Customer Designated POC will be the main point of contact specified in the Order Form, unless Customer designates a security, privacy, or incident-response contact in writing through Sierra's then-current notice process. Customer is responsible for keeping its Designated POC current. The Sierra Designated POC will be privacy@sierra.ai.

EXHIBIT A TO THE DATA PROCESSING ADDENDUM

This Exhibit A forms part of the Addendum and supplements the Standard Contractual Clauses. Capitalized terms not defined in this Exhibit A have the meaning set forth in the Addendum.

The Parties agree that the following terms will supplement the Standard Contractual Clauses:

- 1. Supplemental Terms.** The Parties agree that: (i) a new Clause 1(e) is added to the Standard Contractual Clauses which will read: “To the extent applicable, these Clauses also apply, with the necessary modifications, to the Parties’ processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities will be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.”; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which will read: “To the extent applicable, these Clauses, as supplemented by Annex III, also apply, with the necessary modifications, to the Parties’ processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III).”; (iii) the optional text in Clause 7 is deleted; (iv) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer must notify data exporter of any new Subprocessors in accordance with Section 3(d) of the Addendum; (v) the optional text in Clause 11 is deleted; and (vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).
- 2. Annex I.** Annex I to the Standard Contractual Clauses will read as follows:

A. List of Parties

Data Exporter: Customer.

Address: As set forth in the Order Form.

Contact person’s name, position, and contact details: Customer’s Designated POC.

Activities relevant to the data transferred under these Clauses: The Platform Services.

Role: Controller.

Data Importer: Sierra.

Address: 150 Sutter Street, #690, San Francisco, CA 94104

Contact person’s name, position, and contact details: Sierra’s Designated POC.

Activities relevant to the data transferred under these Clauses: The Platform Services.

Role: Processor.

B. Description of the Transfer:

Categories of data subjects whose personal data is transferred: The categories of data subjects whose personal data is transferred under the Standard Contractual Clauses including, but not limited to, Customer and Customer’s employees, contractors and end users.

Categories of personal data transferred: The categories of personal data transferred under the Standard Contractual Clauses including, but not limited to, any Personal Data included in the Customer Personal Data, including business contact information (names and emails) from Customer’s employees and contractors, and Personal Data included in order and transaction information from Customer’s end users Processed via the Platform Services.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: Sensitive data that is transferred under the Standard Contractual Clauses, including, any sensitive data that Customer’s

end users submit for processing via the Platform Services. Sierra will only Process such sensitive data to provide the Platform Services pursuant to the Agreement.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is transferred in accordance with the standard functionality of the Platform Services, or as otherwise agreed upon by the Parties.

Nature of the processing: The Platform Services.

Purpose(s) of the data transfer and further processing: The Platform Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Data importer will retain personal data in accordance with the Addendum.

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

A list of Sierra's Subprocessors is available as set out in Section 3(d) of the Addendum.

C. Competent Supervisory Authority: The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the Parties consistent with the conditions set forth in Clause 13.

D. Clarifying Terms: The Parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses will be provided upon data exporter's written request; (ii) the measures data importer is required to take under Clause 8.6(c) of the Standard Contractual Clauses will only cover data importer's impacted systems; (iii) the audit described in Clause 8.9 of the Standard Contractual Clauses will be carried out in accordance with Section 6 of the Addendum; (iv) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Standard Contractual Clauses will be limited to the termination of the Standard Contractual Clauses; (v) unless otherwise stated by data importer, data exporter will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Standard Contractual Clauses; (vi) the information required under Clause 15.1(c) of the Standard Contractual Clauses will be provided upon data exporter's written request; and (vii) notwithstanding anything to the contrary, data exporter will reimburse data importer for all costs and expenses incurred by data importer in connection with the performance of data importer's obligations under Clause 15.1(b) and Clause 15.2 of the Standard Contractual Clauses without regard for any limitation of liability set forth in the Agreement.

3. Annex II. Annex II of the Standard Contractual Clauses will read as follows:

Data importer will implement and maintain reasonable technical and organizational measures designed to protect personal data in accordance with the Addendum, including as set forth through the Security Exhibit accessible through its Trust Center, a current version attached hereto as Exhibit B.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the Addendum.

4. Annex III. A new Annex III will be added to the Standard Contractual Clauses and will read as follows:

The [UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses](#) ("UK Addendum") is incorporated herein by reference. The reference to the UK Addendum includes any successor or updated version made available by the UK Information Commissioner's Office and incorporated as described in this Exhibit A, to the extent required or permitted under UK Data Protection Laws.

Table 1: The start date in Table 1 is the effective date of the Addendum. All other information required by Table 1 is set forth in Annex I, Section A of the Standard Contractual Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to and is effective as of the effective date of the Addendum. The Modules are as set out in Section 5(d) and the options in Table 2 in relation to Clauses 7, 9(a) and 11 of the Approved EU Standard Contractual Clauses are as set out in paragraphs 1(iii), 1(iv), and 1(v) of Exhibit A.

Table 3: The information required by Table 3 is set forth in Annex I and II to the Standard Contractual Clauses.

Table 4: The Parties agree that Importer may end the UK Addendum as set out in Section 19.

EXHIBIT B - SECURITY EXHIBIT

This Security Exhibit forms part of the written agreement between Sierra and Customer for the Platform Services that references this document (“**Agreement**”). Capitalized terms not defined in this Security Exhibit have the meaning set forth in the Agreement or the Data Processing Addendum (“**Addendum**” or “**DPA**”), as applicable.

Sierra maintains a written information security program that is designed to safeguard Sierra’s systems and Customer Materials. This Security Exhibit describes the information security program and safeguards that Sierra maintains with respect to the handling of Customer Materials.

1. **ACCESS CONTROLS.** The Platform Services consist of a multi-tenant, software-as-a-service architecture designed to isolate and restrict Customer Materials. Sierra logically isolates Customer Materials based on a unique tenant identifier. Further, Sierra has implemented measures and policies designed to limit access to Customer Materials only to those individuals who have a business need based on role following the least-privilege principle. Sierra has in place processes and tools to create, assign, manage, and revoke access based on authorization. Sierra implements strict controls for access to production deployments, including revoking access for terminated personnel. Sierra requires its personnel to use unique usernames and passwords pursuant to its password policy, including for production network authentication, and requires the use of multi-factor authentication when appropriate, such as for access to production and other privileged systems. Sierra protects access to Customer Materials by implementing mobile device management that permits the secure configuration and management of user endpoints, including enforcing disk encryption, mandatory anti-malware and virus protection, and data loss protection.
2. **SECURITY AUDITS.** Sierra maintains a SOC 2 Type II audit report and ISO 27001 certification from an industry-accredited auditor. Sierra will allow audits subject to the reasonable limitations of the DPA and applicable DORA Addendum (if any). Upon written request, Customer may access a copy of such report through Sierra’s [Trust Center](#).
3. **SECURITY MONITORING.** Sierra logs activity within the Platform Services such as errors and security events to monitor activities which may potentially impact Sierra’s ability to securely provide the Platform Services. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering.
4. **INTRUSION DETECTION.** Sierra, or a third party appointed by Sierra, will provide continuous monitoring of Sierra’s network for unauthorized intrusions. Sierra may collect data through this monitoring about users’ web browsers, *e.g.*, device information such as screen resolution, type, browser, and other such information, for security and fraud detection purposes.
5. **HARDENING.** Sierra hardens the networks and systems supporting the Platform Services based on documented and industry-standard hardening standards that are reviewed at least annually.
6. **ENCRYPTION.** Sierra encrypts all Customer Materials in transit to or from the Platform Services over public networks and at rest, including for backups, using industry standard encryption technologies. Sierra leverages a cloud-based service backed by hardware security modules for the secure key management and key rotation.
7. **VULNERABILITY MANAGEMENT.** Sierra has developed a plan to regularly assess and track vulnerabilities on all enterprise assets within the enterprise’s infrastructure. Sierra monitors public and private industry sources for new threat and vulnerability information and performs vulnerability scans on external-facing systems on at least a quarterly basis. Sierra has in place formal policies to manage vulnerabilities in a timely manner based on risk, including tracking critical and high vulnerabilities to remediation based on industry standards.
8. **ASSET MANAGEMENT.** Sierra has developed and maintains an inventory and an information classification scheme to ensure data is handled according to its sensitivity level.
9. **INCIDENT RESPONSE.** Sierra has established a written incident response policy (“**IRP**”) and program to detect and respond to a confirmed Security Incident, and notify Customer in accordance with the DPA. Sierra communicates its IRP to authorized

individuals and tests its IRP on at least an annual basis. In the event of a Security Incident, Sierra will reasonably cooperate with an impacted Customer to provide it with regular updates on the status of such Security Incident and any remedial actions taken to mitigate the impact.

10. **AVAILABILITY.** Sierra will make the system available as set forth in its Service Level Agreement agreed to with Customer. Sierra has implemented reasonable safeguards to ensure availability for its cloud infrastructure including continuous service level monitoring.
11. **BUSINESS CONTINUITY & DISASTER RECOVERY.** Sierra maintains a documented business continuity and disaster recovery plan (“**BC-DR Plan**”) and tests such BC-DR Plan annually. As part of its BC-DR Plan, Sierra: (a) performs automated backups; (b) has formal processes in place to check business continuity in the event of a disruption; and (c) has formal processes in place to address a disruption to the Platform Services, including the recovery of Customer Materials. Sierra replicates production data to a secondary region in real-time and performs periodic backups for production data.
12. **PHYSICAL SECURITY.** The Platform Services are hosted within the infrastructure provided by Sierra’s cloud provider, which is currently AWS. All physical security controls for the Platform Services are managed by AWS. Sierra’s corporate offices do not host any compute or storage for the Platform Services. Only Sierra employees, contractors, and vendors with regular facilities access will be issued an access card and permitted to physically access Sierra’s corporate offices without escort. Sierra personnel are not permitted to loan out an access card to anyone. Sierra employees, contractors, and vendors are responsible for the badge issued to them, and its use. The physical location of the offices is monitored by 24x7 CCTV cameras.
13. **BACKGROUND CHECKS.** To the extent permitted under law, Sierra performs background checks on all personnel with access to Customer Materials.
14. **SECURITY TRAINING.** Sierra requires its personnel to complete security training upon hire and annually thereafter. All Sierra personnel are required to acknowledge their responsibilities by reviewing and agreeing to Sierra’s written information security policy.
15. **PENETRATION TESTING.** Sierra engages third parties to conduct penetration testing and provide a report of such findings on at least an annual basis. Upon written request, Customer may access a copy of such report through Sierra’s Trust Center.
16. **SECURE DEVELOPMENT.** Sierra has implemented a Secure Development Policy (“**SDP**”) to govern the development, acquisition, implementation, changes, and maintenance of applicable systems and technology within the Platform Services. Sierra logically separates production environments from development environments. The SDP includes formal change control procedures, documented peer reviews, pre-production testing, and appropriate segregation of duties.
17. **DELETION AND EXIT MANAGEMENT.** Sierra has in place formal processes for the secure deletion of Customer Materials upon termination of the Agreement. Such deletion will be carried out in accordance with industry best practices, including appropriate technical means to enable return or export of Customer Personal Data and critical Customer Materials to support Customer’s business continuity and compliance with Data Protection Laws.
18. **SUBPROCESSOR RISK MANAGEMENT.** Sierra conducts reasonable diligence on the privacy and security measures of its Subprocessors to ensure that each Subprocessor maintains security measures consistent with Sierra’s obligations in the Agreement. Customer’s rights with respect to Subprocessors are discussed in the DPA. Sierra provides notice and information about the Subprocessors supporting the Platform Services in the Sierra [Trust Center](#).
19. **CUSTOMER RESPONSIBILITIES.** Sierra has designed the Platform Services with the assumption that certain controls will be the responsibility of the Customer. The following is a representative list of controls that are recommended to be used to reduce risk and enhance security when using the Platform Services:

- a. Customer is responsible for ensuring only authorized personnel have access rights to the Sierra Platform Services, as relevant to their role, *e.g.*, administrative or end-user.
- b. Customer is responsible for securely deploying client-side integrations interfacing with the Platform Services.
- c. Customer is responsible for validating the accuracy, completeness, and legality of Customer Materials and Input submitted in Customer's environment, in compliance with Data Protection Laws.
- d. Customer is responsible for data confidentiality controls within its organization, such as segregation of duties, and non-disclosure of information within its organization.
- e. Customer is responsible for alerting Sierra of security incidents of which Customer becomes aware.
- f. Customer is responsible for implementing appropriate access controls for any systems it chooses to integrate with the Sierra Platform Services.
- g. Customer is responsible for ensuring that Inputs do not violate, or intend to direct the Platform Services to violate, this Agreement or Data Protection Laws.
- h. Customer is responsible for determining whether the use of the Platform Services is appropriate for the storage and Processing of Customer Personal Data, in compliance with Data Protection Laws.

20. **SERVICE OPTIMIZATION.** Sierra may Process Input, Output, and Customer Materials, including Personal Data, to: (i) detect, prevent, investigate, and remediate Security Incidents; (ii) protect against fraudulent or illegal activity; and (iii) provide and improve the Platform Services in accordance with the Agreement and Customer's documented instructions.

Last Updated: November 15, 2024

ACCEPTABLE USE POLICY

This Acceptable Use Policy (“AUP”) identifies prohibited uses of our customer service AI agents (“Services”) made available to you. We or our service providers may update the AUP upon fifteen (15) days’ notice to you. We do not allow the Services to be used for the following:

Deceptive or misleading activities. This includes using the Services to:

- Impersonate a human by presenting results as human-generated, or using results in a manner intended to convince a natural person that they are communicating with a natural person;
- Engage in coordinated inauthentic behavior or disinformation campaigns;
- Generate deceptive or misleading comments or reviews;
- Plagiarize or engage in other forms of academic dishonesty.

Abusive or fraudulent activities. This includes using the Services to:

- Attempt to override or circumvent safety filters or intentionally direct the product or service to act in a manner that contravenes our policies (including this AUP);
- Promote or facilitate the generation or distribution of spam;
- Generate content for fraudulent activities, scams, phishing or malware;
- Compromise security or gain unauthorized access to computer systems or networks, including spoofing and social engineering;
- Violate any natural person’s rights, including privacy rights as defined in applicable privacy law;
- Track or monitor an individual without their consent;
- Inappropriately use confidential or personal information;
- Interfere with or negatively impact our or our service providers’ products or services;
- Utilize input or output of our Services to train an AI model or have an AI model trained (e.g., “model scraping”).

Illegal, malicious or highly regulated activities. This includes using the Services to:

- Engage in, promote, generate, contribute to, encourage, plan, incite, or further illegal or unlawful activity or content;
- Provide instructions on how to create or facilitate the exchange of illegal substance or goods;
- Encourage or provide instructions on how to engage in or facilitate illegal services such as human trafficking or prostitution;
- Design, market, or distribute weapons, explosives, or other dangerous materials;
- Provide instructions on how to commit, facilitate or encourage any type of crime.

Activities with a high risk of economic harm. This includes using the Services to:

- Engage in multi-level marketing or pyramid schemes;
- Gamble or bet on sports;
- Engage in payday lending activities;
- Automate determinations about the eligibility of individuals for financial products, creditworthiness, public assistance services, or decisions regarding eligibility for housing, including leases and home loans;
- Automate determinations about the admissibility of individuals to educational institutions, or the employability of individuals or other employment determinations.

Violent, hateful, or threatening activities. This includes using the Services to:

- Further violent extremism;
- Describe, encourage, support, or provide instructions on how to commit violent acts against persons (including self-harm), animals, or property;
- Encourage hate speech or discriminatory practices that could cause harm or adverse impact to individuals or communities based on their protected attributes, such as race, ethnicity, religion, nationality, gender, sexual orientation, or any other identifying trait.
- Encourage or engage in any form of self-harm;
- Shame, humiliate, bully, celebrate the suffering of, or harass individuals.

Sexually explicit activities. This includes using the Services to:

- Generate pornographic content or content meant for sexual gratification, including activity that describes sexual intercourse, sexual acts, or sexual fetishes, or promotes sexual services (excluding sex education and wellness);
- Engage in erotic chats.

Child sexual exploitation or abuse activities. We strictly prohibit and will report to relevant authorities and organizations where appropriate any activity or content that exploits or harms children, or describes, encourages, supports or promotes any form of child sexual exploitation or abuse in addition to Child Sexual Abuse Material (CSAM).

If you have any questions about whether your activity or use case is permitted or prohibited by this AUP, please email support@sierra.ai.