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**."

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.