

Google Cloud Terms of Service for G-Cloud 15 - Lot 3

1. General Terms applicable to the Digital Platform (G-Cloud 15)

- 1.1. General. These terms and conditions (“Agreement”) govern the Buyer’s use of the Services purchased under Lot 3 via the Digital Platform and contracted for under the G-Cloud 15 Framework Agreement and G-Cloud 15 Call-Off Contract.
- 1.2. Use of the Services. Notwithstanding any provision to the contrary in this Agreement, if the Buyer uses a service which does not form part of the Services purchased under a G-Cloud 15 Call-Off Contract (“Out of Scope Services”), the Buyer understands that it will not be able to use the Out of Scope Services under the terms of the G-Cloud 15 Framework Agreement and G-Cloud 15 Call-Off Contract. If the Buyer wishes to use the Out of Scope Services, then where the Out of Scope Services are:
 - 1.2.a. available on the Digital Platform, the Parties will need to agree and enter into a separate G-Cloud 15 Call-Off Contract governed by the G-Cloud 15 Framework Agreement; or
 - 1.2.b. not available on the Digital Platform, the Buyer understands that use of the Out of Scope Services will be outside of the Digital Platform (and this procurement process) and subject to the Supplier’s standard terms for the relevant Out of Scope Services. For example, if it is a Google Cloud Platform service, the terms available here: <https://cloud.google.com/terms/> will apply.
- 1.3. Prices. The Framework Prices for the Services are set out on the Digital Platform. If a Buyer selects different pricing and discounts through the functionality of the Services, then the Buyer understands that such activity is outside of the G-Cloud 15 Call-Off Contract terms (and this procurement process).
- 1.4. Conflict of provisions. It is acknowledged that where there is a conflict and/or inconsistency in relation to this Agreement and the other documents comprising the Supplier’s relationship with the Buyer under G-Cloud 15, the order of precedence will be as set out in the G-Cloud 15 Call-Off Contract.
- 1.5. Governing Law. It is acknowledged that the Agreement is governed by English law as further set out in clause 39 of the General Terms incorporated into the G-Cloud 15 Call-Off Contract and the Parties submit to the exclusive jurisdiction of the English courts in relation to any dispute (contractual or non-contractual) concerning the Agreement, but either Party

may apply to any court for an injunction or other relief to protect its Intellectual Property Rights.

- 1.6. Reference Documentation. The (i) Implementation Services Agreement, (ii) Cloud Data Processing Addendum (Customers), (iii) Google Cloud Acceptable Use Policy, (iv) Generative AI Prohibited Use Policy, (v) Abuse Monitoring, (vi) SecOps Services Summary, (vii) SecOps Service Specific Terms, and (viii) Google Cloud Training Terms of Service are included in this document for reference only. To the extent there are any support services provided in conjunction with Lots 1 and/or 2, the applicable support terms outlined in Lots 1 and/or 2 shall apply including Google Cloud Support Services Technical Support Services Guidelines (<https://cloud.google.com/terms/tssg>).
- 1.7. Licence to Use. The licence that the Supplier gives to the Buyer as referred to in clause 10 of the General Terms incorporated into the G-Cloud 15 Call-Off Contract, shall be a reference to the right to access the Services as referred to in the applicable Supplier Licence Terms in the Order Form and shall not constitute a licence by the Supplier to the Buyer.
- 1.8. Interpretation. When interpreting this Agreement, references to:
 - 1.8.a. Customer means Buyer (as defined in the G-Cloud 15 Call-Off Contract);
 - 1.8.b. Google means Supplier (as defined in the G-Cloud 15 Call-Off Contract);
 - 1.8.c. Effective Date means the Start Date (as defined in the G-Cloud 15 Call-Off Contract);
 - 1.8.d. Services means the Services, Cloud Support Services and Additional Services (each as defined in the G-Cloud 15 Call-Off Contract and covering Lot 3 services only); and these Lot 3 Services include specified work product “Deliverables” (as defined by Google), but for the avoidance of doubt are not to be interpreted as any type of Deliverable (as defined in the G-Cloud 15 Call-Off Contract) other than Services;
 - 1.8.e. “Third Party Offerings” (as defined by Google) are excluded from Software, COTS Software and Cloud Products (each as defined in the G-Cloud 15 Call-Off Contract, to the extent relevant to Lot 3 Services);

- 1.8.f. where specified in the Call-Off Contract, Software (as defined in the G-Cloud 15 Call-Off Contract) means “Premium Software” (as defined in Google’s Service Specific Terms);
- 1.8.g. to the extent applicable to some of the Deliverables (as defined in the G-Cloud 15 Call-Off Contract) under the relevant Order Form and/or Call-Off Contract, the licence that the Supplier gives to the Buyer as referred to in clause 10 of the General Terms and/or Call-Off Schedule 1 incorporated into the G-Cloud 15 Call-Off Contract shall be a reference to Cloud Products (as defined in the G-Cloud 15 Call-Off Contract) licensed under the applicable Supplier Licence Terms in the Order Form;
- 1.8.h. in respect of the Supplier Data Processing Addendum (or Supplier DPA) and in all other respects, for the avoidance of doubt, Services does not include or constitute Software (each as defined in the G-Cloud 15 Call-Off Contract); and
- 1.8.i. Term means the Term (as defined in the G-Cloud 15 Call-Off Contract).

Contents

1. Implementation Services Agreement
2. Cloud Data Processing Addendum (Customers)
 - a. General Terms
 - b. Appendix 1: Subject Matter and Details of Data Processing
 - c. Appendix 2: Security Measures
 - d. Appendix 3: Specific Privacy Laws
 - e. Appendix 4: Specific Products
3. Google Cloud Acceptable Use Policy
4. Generative AI Prohibited Use Policy
5. Abuse Monitoring
6. SecOps Services Summary
7. SecOps Service Specific Terms
 - a. General Service Terms
 - b. Service Terms
 - c. Partner-Specific Terms
 - d. Google Cloud Platform Terms
8. Google Cloud Training Terms of Service

Implementation Services Agreement

To receive the Services described below, Customer agrees to the terms of this Implementation Services Agreement, including any Regional Terms below (the “Agreement”). Together with any applicable Order Form, the Agreement governs Customer’s receipt of Services from Google. “Google” has the meaning given at <https://cloud.google.com/terms/google-entity>.

1. Services

1.1 Services. Google will provide Services, including Deliverables, to Customer in accordance with the Agreement, subject to Customer fulfilling its obligations under Section 2.1 (Cooperation).

1.2 Change Orders. Any changes to an Order Form require a written amendment signed by Customer and Google.

1.3 Personnel. Google will determine which Personnel will perform the Services. If Customer requests a change of Personnel and provides a reasonable and legal basis for such request, Google will use commercially reasonable efforts to replace the assigned Personnel with alternative Personnel.

1.4 Subcontracting. Google may subcontract any of its obligations under the Agreement but will remain liable to Customer for any subcontracted obligations.

1.5 Compliance with Customer’s Onsite Policies and Procedures. If provided to Google in writing before the start of the Services, Google’s Personnel performing Services will comply with: (i) Customer’s reasonable personnel training policies related to the Services and (ii) for Services performed at Customer’s facilities, Customer’s reasonable written onsite policies and procedures.

2. Customer Obligations.

2.1 Cooperation. Customer will provide reasonable and timely cooperation in connection with Google’s provision of the Services. Google will not be liable for a delay caused by Customer’s failure to provide Google with information, materials, consents or access to Customer facilities, networks or systems required for Google to perform the Services. If Google informs Customer of such failure and Customer does not cure the failure within 30 days, then: (a) Google may terminate any incomplete Services and (b) in addition to any fees due under Section 7.4(b) (Effect on Payment), Customer will pay actual costs incurred by Google for the cancelled Services, provided Google will make commercially reasonable efforts to mitigate those costs, which will not exceed the Fees.

2.2 Consents. Customer is responsible for any consents and notices required to permit Customer’s use and receipt of the Services.

2.3 No Personal Data. Customer acknowledges that Google does not need to process Personal Data to perform the Services. Customer will not provide Google with access to Personal Data unless the parties have agreed in a separate agreement on the scope of work and any terms applicable to Google’s processing of such Personal Data.

3. Payment Terms.

3.1 Payment. Customer will pay all Fees for Services ordered under the Agreement. Google will invoice Customer for the Fees. Customer will pay all invoiced amounts by the Payment Due Date. All payments are due in the currency described in the

invoice. Wire transfer payments will include the bank information described in the invoice. Unless required by law, Fees for some Services may be non-cancellable, as specified on an Order Form.

3.2 Taxes. Google will itemize any invoiced Taxes. Customer will pay invoiced Taxes unless Customer provides a valid tax exemption certificate. Customer may withhold Taxes if Customer provides a valid receipt evidencing the taxes withheld.

3.3 Invoice Disputes. Customer will submit any invoice disputes in good faith to collections@google.com before the Payment Due Date. If the parties determine that Fees were incorrectly invoiced, Google will issue a credit equal to the agreed amount.

3.4 Overdue Payments.

a. Customer's payment of Fees is overdue if Google has not received it by the Payment Due Date. If Customer's payment is overdue, except for amounts subject to an Invoice Dispute submitted before the Payment Due Date, Google may (i) charge interest on overdue amounts at 1.5% per month (or the highest rate permitted by law, if less) from the Payment Due Date until paid in full, and (ii) Suspend the Services.

b. Customer will reimburse Google for all reasonable expenses (including attorneys' fees) incurred by Google in collecting overdue payments except where such payments are due to Google's billing inaccuracies.

3.5 Expenses. Customer will reimburse expenses:

a. as specifically described in the applicable Order Form; or

b. up to the amounts specified as "expenses" in the applicable Order Form that are actual, reasonable, and necessary.

3.6 Partner Orders. If Customer orders Services from a Partner: (a) Customer will pay the Partner for the Services under payment terms agreed to between Customer and the Partner, (b) Sections 3.1-3.5 (Payment) of the Agreement will not apply to the Services, and (c) Google will not owe any credits or refunds for the Services to Customer. Customer may obtain credits or refunds for the Services from the Partner to the extent agreed to between Customer and the Partner.

4. Intellectual Property.

4.1 Background IP. Customer owns all rights, title and interest in Customer's Background IP. Google owns all rights, title and interest in Google's Background IP. Customer grants Google a license to use Customer's Background IP to provide the Services (with a right to sublicense to Google Affiliates and subcontractors). Except for the license rights under Sections 4.2 (Google Technology) and 4.3 (Deliverables), neither party will acquire any right, title, or interest in or to the other party's Background IP under the Agreement.

4.2 Google Technology. Google owns all rights, title and interest in Google Technology. To the extent Google Technology is incorporated into Deliverables, Google grants Customer a limited, worldwide, non-exclusive, perpetual, non-transferable license to use the Google Technology in connection with the Deliverables for Customer's internal business purposes.

4.3 Deliverables. Google grants Customer a limited, worldwide, non-exclusive, perpetual, non-transferable license to use, reproduce and modify the Deliverables for Customer's internal business purposes.

4.4 Feedback. At its option, Customer may provide feedback and suggestions about the Services to Google ("Feedback"). If Customer provides Feedback, then Google

and its Affiliates may use that Feedback without restriction and without obligation to Customer.

5. Confidentiality.

5.1 Confidentiality Obligations. Subject to Section 5.2 (Disclosure of Confidential Information), the recipient will use the other party's Confidential Information only to exercise its rights and fulfill its obligations under the Agreement. The recipient will use reasonable care to protect against disclosure of the other party's Confidential Information to parties other than the recipient's employees, Affiliates, agents, or professional advisors ("Delegates") who need to know it and who have a legal obligation to keep it confidential. The recipient will ensure that its Delegates are also subject to the same non-disclosure and use obligations.

5.2 Disclosure of Confidential Information.

a. **General.** Regardless of any other provision in the Agreement, the recipient and its Delegates may disclose the other party's Confidential Information (i) with the other party's written consent or (ii) in accordance with a Legal Process request, subject to Section 5.2(b) (Legal Process Notification).

b. **Legal Process Notification.** The recipient will use commercially reasonable efforts to notify the other party before disclosing that party's Confidential Information in accordance with Legal Process. Notice is not required before disclosure if the recipient is informed that (i) it is legally prohibited from giving notice or (ii) the Legal Process relates to exceptional circumstances involving danger of death or serious physical injury.

c. **Opposition.** The recipient will, and will ensure that its Delegates will, comply with the other party's reasonable requests to oppose disclosure of its Confidential Information.

5.3 Marketing and Publicity. Each party may use the other party's Brand Features in connection with the Agreement as permitted in the Agreement. Customer may state publicly that it is a Google customer and display Google Brand Features in accordance with the Trademark Guidelines. Customer and Google will work together on an announcement of Customer being a Google customer, which will take place on an agreed upon date within 6 months of the Effective Date. Additionally, with prior written consent, the parties may engage in joint marketing activities such as customer testimonials, press engagements, public speaking events, and analyst interviews. A party may revoke the other party's right to use its Brand Features with 30 days' written notice. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features.

6. Warranties and Remedies.

6.1 Mutual Warranty. Each party represents and warrants that it has full power and authority to enter into the Agreement.

6.2 Google Warranty. Google will perform the Services in a professional and workmanlike manner, in accordance with practices used by other service providers performing services similar to the Services. Google will use Personnel with the requisite skills, experience, and qualifications to perform the Services. Any claim that Google has breached this warranty will be made within 30 days after Google has provided the Services, subject to applicable law.

6.3 Remedies. Subject to applicable law, Google's entire Liability and Customer's sole remedy for Google's failure to provide Services that conform with Section 6.2 (Google Warranty) will be for Google to at its option: (1) use commercially

reasonable efforts to re-provide the Services or (2) terminate the Order Form and refund any applicable Fees received for the nonconforming Services.

6.4 Disclaimer. Except as expressly provided for in the Agreement, to the fullest extent permitted by applicable law, Google does not make any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, fitness for a particular use, noninfringement, or error-free or uninterrupted use of the Services.

7. Term; Termination.

7.1 Agreement Term. The Agreement will start on the Effective Date and continue until the expiration or termination of the Order Form.

7.2 Termination for Convenience. Subject to any financial commitments in an Order Form or addendum to the Agreement, Customer may terminate the Agreement or an Order Form for any reason with 30 days' prior written notice to Google.

7.3 Termination for Breach.

a. Termination of an Order Form. Either party may terminate an Order Form if the other party is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written notice.

b. Termination of the Agreement. Either party may terminate the Agreement if the other party: (i) is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written notice; (ii) ceases its business operations or to the extent permitted by applicable law, becomes subject to insolvency proceedings and such proceedings are not dismissed within 90 days; or (iii) an applicable law or government order prohibits the provision of the Services.

7.4 Effects of Termination. If the Agreement terminates or expires, then unless otherwise agreed in writing between the Parties, all Order Forms also terminate or expire. The termination or expiration of one Order Form will not affect other Order Forms. If an Order Form terminates or expires, then:

a. Effect on Services. The rights under the Agreement granted by one party to the other regarding the Services will cease immediately except as described in this Section 7.4 (Effects of Termination); and Google will stop work on the Services and at Customer's request provide any work-in-progress Deliverables to Customer;

b. Effect on Payment. Customer will pay for: (i) Services, including work-in-progress, performed before the effective date of termination or expiration and (ii) except as required by law, any remaining non-cancellable Fees. Google will send Customer a final invoice for payment obligations under the Order Form.

c. Survival. The following Sections of the Agreement will survive expiration or termination of the Agreement: 3 (Payment Terms), 4 (Intellectual Property), 5 (Confidentiality), 6.3 (Remedies), 6.4 (Disclaimer), 7.4 (Effects of Termination), 8 (Indemnification), 9 (Liability), 11 (Miscellaneous), and 12 (Definitions).

8. Indemnification.

8.1 Google Indemnification Obligations. Google will defend Customer against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that Customer's use of Google Indemnified Materials in accordance with the Agreement infringes the third party's Intellectual Property Rights.

8.2 Customer Indemnification Obligations. Customer will defend Google, its Personnel, and its Affiliates, and indemnify them against Indemnified Liabilities in

any Third-Party Legal Proceeding to the extent arising from any Customer Indemnified Materials.

8.3 Indemnification Exclusions. Sections 8.1 (Google Indemnification Obligations) and Section 8.2 (Customer Indemnification Obligations) will not apply to the extent the underlying allegation arises from:

- a. the indemnified party's breach of the Agreement; or
- b. modifications to the Google Indemnified Materials or Customer Indemnified Materials (as applicable) by anyone other than the indemnifying party; or
- c. combination of the Google Indemnified Materials or Customer Indemnified Materials (as applicable) with materials not provided by the indemnifying party under the Agreement; or
- d. compliance with the indemnified party's instructions, design or request for customized features.

8.4 Indemnification Conditions. Sections 8.1 (Google Indemnification Obligations) and 8.2 (Customer Indemnification Obligations) are conditioned on the following:

- a. The indemnified party will promptly notify the indemnifying party in writing of any allegation(s) that preceded the Third-Party Legal Proceeding and cooperate reasonably with the indemnifying party to resolve the allegation(s) and Third-Party Legal Proceeding. If breach of this Section 8.4(a) prejudices the defense of the Third-Party Legal Proceeding, the indemnifying party's obligations under Section 8.1 (Google Indemnification Obligations) or 8.2 (Customer Indemnification Obligations) (as applicable) will be reduced in proportion to the prejudice.
- b. The indemnified party will tender sole control of the indemnified portion of the Third-Party Legal Proceeding to the indemnifying party, subject to the following: (i) the indemnified party may appoint its own non-controlling counsel, at its own expense; and (ii) any settlement requiring the indemnified party to admit liability, pay money, or take (or refrain from taking) any action, will require the indemnified party's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

8.5 Remedies.

- a. If Google reasonably believes the Services or Deliverables might infringe a third party's Intellectual Property Rights, then Google may, at its sole option and expense: (i) procure the right for Customer to continue using the Services or Deliverables; (ii) modify the Services or Deliverables to make them non-infringing without materially reducing their functionality; or (iii) replace the Services or Deliverables with a non-infringing, functionally equivalent alternative.
- b. If Google does not believe the remedies in Section 8.5(a) (Remedies) are commercially reasonable, then Google may (i) terminate the impacted Services and Customer's use of the impacted Deliverables and (ii) provide a pro-rated refund of any Fees paid for such Services or Deliverables.

8.6 Sole Rights and Obligations. Without affecting either party's termination rights, and to the extent permitted by applicable law, this Section 8 (Indemnification) states the parties' sole and exclusive remedy under the Agreement for any third party allegations of Intellectual Property Rights infringement covered by this Section 8 (Indemnification).

9. Liability.

9.1 Limited Liabilities.

a. To the extent permitted by applicable law and subject to Section 9.2 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Agreement for any:

- i. indirect, consequential, special, incidental, or punitive damages; or
- ii. lost revenues, profits, savings, or goodwill.

b. Each party's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the Fees Customer paid under the Order Form.

9.2 Unlimited Liabilities. Nothing in the Agreement excludes or limits either party's Liability for:

- a. death, personal injury, or tangible personal property damage resulting from its negligence or the negligence of its employees or agents;
- b. its fraud or fraudulent misrepresentation;
- c. its obligations under Section 8 (Indemnification);
- d. its infringement of the other party's Intellectual Property Rights;
- e. its payment obligations under the Agreement; or
- f. matters for which liability cannot be excluded or limited under applicable law.

10. Insurance.

During the term of the Agreement, each party will maintain, at its own expense, appropriate insurance coverage applicable to performance of the party's respective obligations under the Agreement, such as general commercial liability, worker's compensation, automobile liability, and professional liability.

11. Miscellaneous.

11.1 Notices. Google will provide notice to Customer under the Agreement by sending an email to the Notification Email Address. Customer will provide notice to Google by sending an email to legal-notices@google.com. Notice will be treated as received when the email is sent. Customer is responsible for keeping its Notification Email Address current throughout the Term.

11.2 Emails. The parties may use emails to satisfy written approval and consent requirements under the Agreement.

11.3 Assignment. Neither party may assign the Agreement without the written consent of the other, except Google may assign the Agreement to an Affiliate where: (a) the Affiliate will be responsible for Google's obligations under the Agreement; and (b) Google has notified the Customer of the assignment. Any other attempt to assign is void.

11.4 Change of Control. If a party experiences a change of Control other than an internal restructuring or reorganization: (a) that party will give written notice to the other party within 30 days after the change of Control; and (b) the other party may immediately terminate the Agreement any time within 30 days after it receives that written notice.

11.5 Force Majeure. Neither party will be liable for failure or delay in performance of its obligations to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war.

11.6 *No Agency*. The Agreement does not create any agency, partnership, or joint venture between the parties or the relationship of employer and employee between: (a) the parties, or (b) one party and the other party's Personnel.

11.7 *No Waiver*. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Agreement.

11.8 *Severability*. If any part of the Agreement is invalid, illegal or unenforceable, the rest of the Agreement will remain in effect.

11.9 *No Third-Party Beneficiaries*. The Agreement does not confer any benefits on any third party unless it expressly states that it does.

11.10 *Equitable Relief*. Nothing in the Agreement will limit either party's ability to seek equitable relief.

11.11 *Governing Law*. All claims arising out of or relating to the Agreement or the Services will be governed by California law, excluding that state's conflict of laws rules, and will be litigated exclusively in the federal or state courts of Santa Clara County, California; the parties consent to personal jurisdiction in those courts.

11.12 *Amendments*. Except as specifically described otherwise in the Agreement, any amendment to the Agreement will be in writing, expressly state that it is amending the Agreement, and be signed by both parties.

11.13 *Updates*. Google may update the terms of the Agreement from time to time. The terms of the updated Agreement will apply only to Order Forms signed by Customer and Google after Google posts the updated Agreement to a publicly available URL.

11.14 *Independent Development*. Nothing in the Agreement will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs or technology that are similar to the subject of the Agreement, provided that the party does not violate its obligations under the Agreement in doing so.

11.15 *Entire Agreement*. The Agreement states all terms agreed between the parties, and supersedes any prior or contemporaneous agreements between the parties relating to the subject matter of the Agreement. In entering into the Agreement, neither party has relied on, and neither party will have any right or remedy based on, any statement, representation or warranty (whether made negligently or innocently), except those expressly described in the Agreement. Nothing in the Agreement grants any right for Customer to use materials, products or services that are made available to Google customers under a separate license or agreement.

11.16 *Conflicting Terms*. If there is a conflict among the documents that make up the Agreement, then the documents will control in the following order: the applicable Order Form and the Agreement.

11.17 *Conflicting Languages*. If the Agreement is translated into any other language, and there is a discrepancy between the English text and the translated text, the English text will control.

11.18 *Counterparts*. The parties may execute the Agreement in counterparts, including facsimile, PDF, and other electronic copies, which taken together will constitute one instrument.

11.19 *Electronic Signatures*. The parties consent to electronic signatures.

11.20 *Headers*. Headings and captions used in the Agreement are for reference purposes only and will not have any effect on the interpretation of the Agreement.

12. Definitions.

“*Affiliate*” means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.

“*Background IP*” means all Intellectual Property owned or licensed by a party (a) before the Effective Date of the applicable Order Form or (b) independent of the Services.

“*Brand Features*” means each party’s trade names, trademarks, logos, domain names, and other distinctive brand features.

“*Confidential Information*” means information that one party (or an Affiliate) discloses to the other party under the Agreement, and that is marked as confidential or would normally be considered confidential information under the circumstances.

Confidential Information does not include information that is independently developed by the recipient, is shared with the recipient by a third party without confidentiality obligations, or is or becomes public through no fault of the recipient.

“*Control*” means control of greater than 50% of the voting rights or equity interests of a party.

“*Customer Indemnified Materials*” means: (a) Customer Background IP, and any other information, materials, or technology provided to Google by Customer in connection with the Services (in each case, excluding any open source software); and (b) Customer’s Brand Features. Customer Indemnified Materials do not include Google Technology or Deliverables.

“*Customer*” means the Party purchasing Services from Google as identified on an applicable Order Form.

“*Deliverables*” means work product created specifically for Customer by Google Personnel as part of the Services and specified as Deliverables as part of an Order Form.

“*Effective Date*” means the date of the last party’s signature of an Order Form incorporating the Agreement.

“*EU GDPR*” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

“*Fees*” means the applicable fees for the Services as specified in an Order Form, including any reimbursable expenses (if applicable).

“*Google Indemnified Materials*” means (a) Deliverables and Google Technology (in each case, excluding any open source software); or (b) Google’s Brand Features. Google Indemnified Materials do not include Customer Background IP.

“*Google Technology*” means: (a) Google Background IP, (b) all Intellectual Property and know-how applicable to Google products and services, and (c) tools, code, algorithms, modules, materials, documentation, reports and technology developed in connection with the Services that have general application to Google’s other customers, including derivatives of and improvements to Google’s Background IP. Google Technology does not include Customer Background IP or Customer Confidential Information.

“*Including*” or “*including*” means including but not limited to.

“*Indemnified Liabilities*” means any (i) settlement amounts approved by the indemnifying party, and (ii) damages and costs in a final judgment awarded against the indemnified party and its Affiliates by a court of competent jurisdiction.

“*Intellectual Property*” or “*IP*” means anything protectable by an Intellectual Property Right.

“*Intellectual Property Right(s)*” means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

“*Liability*” means any liability, whether under contract, tort (including negligence), or otherwise, regardless of whether foreseeable or contemplated by the parties.

“*Notification Email Address*” means the email address(es) designated by Customer in the applicable Order Form.

“*Order Form*” means an order form or other document issued by Google under the Agreement, including data sheets associated with Services described in the order form, and executed by Customer and Google specifying the Services Google will provide to Customer.

“*Partner*” means a third party authorized by Google to resell the Services.

“*Payment Due Date*” means the payment due date stated in the applicable Order Form, or in its absence, 30 days from the invoice date.

“*Personal Data*” means personal data as defined under any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation or, absent any such meaning or law, by the EU GDPR.

“*Personnel*” means a party’s and its Affiliates’ respective directors, officers, employees, agents, and subcontractors.

“*Services*” means the then-current advisory and implementation services described at g.co/cloudpsoterms (<https://services.google.com/fh/files/misc/cloud-pso-services-list.pdf>) and similar advisory or implementation services designed to help Customer use Google products and services. Services do not include Training Services.

“*Tax(es)*” means all government-imposed taxes, except for taxes based on Google’s net income, net worth, asset value, property value, or employment.

“*Third-Party Legal Proceeding*” means any formal legal proceeding filed by an unaffiliated third party before a court or government tribunal (including any appellate proceeding).

“*Trademark Guidelines*” means Google’s Brand Terms and Conditions, located at: <http://www.google.com/permissions/trademark/brand-terms.html>.

“*Training Services*” means education and certification services related to Google products and services for individual or groups of users described as training at g.co/cloudpsoterms (<https://services.google.com/fh/files/misc/cloud-pso-services-list.pdf>).

13. Regional Terms.

Customer agrees to the following modifications to the Agreement if Customer has a billing address in the locations described below:

Americas

Argentina, Bolivia, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, Nicaragua, Panamá, Paraguay, Puerto Rico, Perú, República Dominicana, Uruguay or Venezuela	1. Sections 4.2 and 4.3 are replaced with the following: 4.2 Google Technology. Google owns all rights, title and interest in Google Technology. To the extent Google Technology is incorporated into Deliverables, Google grants Customer a limited, worldwide, non-exclusive, non-transferable license to the maximum extent permitted by law, to use the Google Technology in connection with the Deliverables for Customer's internal business purposes. 4.3 Deliverables. Google grants Customer a limited, worldwide, non-exclusive, non-transferable license to the maximum extent permitted by law, to use, reproduce and modify the Deliverables for Customer's internal business purposes.
--	---

Canada	1. Section 11.11 (Governing Law) is replaced with: Governing Law. All claims arising out of or relating to the Agreement or the Services will be governed by Ontario law and the applicable laws of Canada, excluding that province's conflict of laws rules, and will be litigated exclusively in the federal or state courts of Ontario located in Toronto, Ontario; the parties consent to personal jurisdiction in those courts.
---------------	---

Mexico

Section 3.2 (Taxes) is replaced with:

2.2 Taxes.

(a) *Tax Invoicing and Payments.* Taxes are not included in the Fees and will be separately itemized on Google's invoices if applicable. Customer will pay correctly-invoiced Taxes unless Customer provides a valid tax exemption certificate. If Customer is required by law to withhold any Taxes from its payments to Google, Customer must provide Google with an official tax receipt or other appropriate documentation to support such withholding.

(b) *Tax Documentation.* Google will timely provide customary tax documentation reasonably requested by Customer and vice versa.

Subsection b. in Section 9.1 (Limited Liabilities) is replaced as follows:

b. To the extent permitted by applicable law, each party's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the Fees Customer paid under the Order Form.

Subsection a. in Section 9.2 (Unlimited Liabilities) is replaced as follows:

9.2 *Unlimited Liabilities.* Nothing in the Agreement excludes or limits either party's Liability for:

a. death, personal injury, or tangible personal property damage resulting from its gross negligence or the gross negligence of its employees or agents;

[...]

Section 11.11 (Governing Law) is replaced as follows:

11.11 *Governing Law & Arbitration.*

(a) *Governing Law.* This Agreement is governed by the laws of the United Mexican States, excluding choice of law rules.

(b) *Arbitration.*

(i) *Definitions.* "Dispute" means any contractual or non-contractual dispute regarding this Agreement, including its formation, validity, subject matter, interpretation, performance, or termination.

(ii) *Settlement.* The parties will try in good faith to settle any Dispute within 30 days after a party receives the first notice regarding the Dispute in accordance with Section 11.1 (Notices). If the parties are unable to resolve the Dispute within this 30-day period, either party may refer the Dispute to arbitration in accordance with Section 11.11 (iii) (Arbitration).

(iii) *Arbitration.* Except as prohibited by applicable law, the parties will refer all Disputes to final, binding arbitration under the rules of the Arbitration rules of the National Chamber of Commerce in Mexico City in force as of this Agreement's Effective Date ("Rules"). The arbitration will be conducted in

Spanish by one arbitrator, mutually selected by the parties, in Mexico City, Mexico, which will be the seat of arbitration.

(iv) *Confidentiality*. The arbitration is Confidential Information (including the arbitration's existence and any oral or written information related to it). However, the parties may disclose to a competent court information necessary to (a) require the aid of the competent courts before or during the arbitral proceeding; or (b) execute any arbitral decision, but only if the confidentiality of those materials is maintained in those judicial proceedings.

(v) *Non-Monetary Relief*. The arbitrator may only issue its award based on law, not in equity, and may not award non-monetary relief.

(vi) *Fees and Expenses*. Each party will bear its own lawyers' and experts' fees and expenses, and the arbitrator's final decision must not include any rulings in this regard.

Section 11.19 (Electronic Signatures) is replaced as follows:

11.19 *Electronic Signatures*. The Parties expressly agree to execute this Agreement electronically and acknowledge that electronic signatures hold the same legal validity and enforceability as handwritten signatures, as recognized by applicable law. The Parties further confirm that the electronic signatures used ensure the reliability, integrity, and inalterability of the document, binding the signature to the Agreement in accordance with applicable law. Each Party is responsible for safeguarding the security of its signature credentials, and the electronically signed Agreement shall be deemed final, complete, and binding.

The definition of "Taxes" under Section 12 (Definitions) is replaced as follows:

12. *Definitions*.

"Taxes" means all government-imposed tax obligations (including taxes, duties, and withholdings), except those based on net income, net worth, asset value, property value, or employment.

Asia Pacific

Asia Pacific - All
regions, excluding
India

Section 3.2 is replaced as follows:

3.2 *Taxes*. Google will itemize any invoiced Taxes. If Taxes must be withheld from any payment to Google, then Customer will increase the payment to Google so that the net amount received by Google is equal to the amount invoiced, without reduction for Taxes.

The definition of “Taxes” under Section 12 (Definitions) is replaced as follows:

“*Taxes*” means all government-imposed taxes, as per the applicable law associated with the rendering and performance of the Services, including but not limited to any duties, customs duties, and any direct or indirect taxes, including any related penalties or interest, except for taxes based on Google's profit.

For purposes of Sections 5.3 (Marketing and Publicity) and 6.4 (Disclaimer), “Google” also includes “Google Affiliates”.

Asia Pacific (all regions excluding Australia, Japan, India, New Zealand, Singapore)

Section 11.11 (Governing Law) is replaced with the following:
11.11 Governing Law; Arbitration.

a. ALL CLAIMS ARISING OUT OR RELATING TO THE AGREEMENT OR ANY RELATED GOOGLE PRODUCTS OR SERVICES (INCLUDING ANY DISPUTE REGARDING THE INTERPRETATION OR PERFORMANCE OF THE AGREEMENT) (“DISPUTE”) WILL BE GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA, USA, EXCLUDING CALIFORNIA’S CONFLICTS OF LAWS RULES.

b. The parties will try in good faith to settle any Dispute within 30 days after the Dispute arises. If the Dispute is not resolved within 30 days, it must be resolved by arbitration by the American Arbitration Association’s International Centre for Dispute Resolution in accordance with its Expedited Commercial Rules in force as of the date of the Agreement (“Rules”).

c. The parties will mutually select one arbitrator. The arbitration will be conducted in English in Santa Clara County, California, USA.

d. Either party may apply to any competent court for injunctive relief necessary to protect its rights pending resolution of the arbitration. The arbitrator may order equitable or injunctive relief consistent with the remedies and limitations in the Agreement.

e. Subject to the confidentiality requirements in Subsection (g), either party may petition any competent court to issue any order necessary to protect that party’s rights or property; this petition will not be considered a violation or waiver of this governing law and arbitration section and will not affect the arbitrator’s powers, including the power to review the judicial decision. The parties stipulate that the courts of Santa Clara County, California, USA, are competent to grant any order under this Subsection (e).

f. The arbitral award will be final and binding on the parties and its execution may be presented in any competent court, including any court with jurisdiction over either party or any of its property.

g. Any arbitration proceeding conducted in accordance with this Section will be considered Confidential Information under the Agreement’s confidentiality section, including (i) the existence of, (ii) any information disclosed during, and (iii) any oral communications or documents related to the arbitration proceedings. The parties may also disclose the information described in this Subsection (g) to a competent court as may be necessary to file any order under Subsection (e) or execute any arbitral decision, but the parties must request that those judicial proceedings be conducted in camera (in private).

- h. The parties will pay the arbitrator's fees, the arbitrator's appointed experts' fees and expenses, and the arbitration center's administrative expenses in accordance with the Rules. In its final decision, the arbitrator will determine the non-prevailing party's obligation to reimburse the amount paid in advance by the prevailing party for these fees. (i) Each party will bear its own lawyers' and experts' fees and expenses, regardless of the arbitrator's final decision regarding the Dispute.
- i. The parties agree that a decision of the arbitrators need not to be made within any specific time period.

Indonesia

If Customer orders Services from PT Google Cloud Indonesia, the Indonesian version of this Agreement is accessible [here](#) and Section 11.17. (Conflicting Languages) is replaced with:

This Agreement is made in the Indonesian and the English language. Both versions are equally authentic. In the event of any inconsistency or different interpretation between the Indonesian version and the English version, the parties agree to amend the Indonesian version to make the relevant part of the Indonesian version consistent with the relevant part of the English version.

A new Section 7.5 is added:

Waiver of Laws. Where applicable, the parties agree that for effectiveness of the termination clauses under the Agreement, to waive any provisions, procedures and operation of any applicable law to the extent that a court order is required for termination of the Agreement.

Australia, Japan, Indonesia, Korea and New Zealand

For Google Australia Pty Ltd., Google Cloud Japan G.K., PT Google Cloud Indonesia, Google Cloud Korea, and Google New Zealand Limited, "Google" means Google Asia Pacific Pte. Ltd. and/or its Affiliates (including Google Australia Pty Ltd., Google Cloud Japan G.K., PT Google Cloud Indonesia, Google Cloud Korea, and Google New Zealand Limited, as applicable) as the context requires.

India

India

1. For Customers who order Services from Google Cloud India Private Limited: (a) except for this Section, the terms of the Agreement do not apply and (b) the terms of the [Implementation Services Agreement India - GCP](#) apply.

Australia

A new Section 6.5 is added as follows:

6.5. This Section 6.5 applies only if the Services are subject to statutory guarantees under the Australian Competition and Consumer Act 2010 (“ACCA”). Applicable laws, including the ACCA, may confer rights and remedies into this Agreement that cannot be excluded, and which are not excluded by this Agreement. To the extent that the applicable laws permit Google to limit their operation, Google’s and its Affiliates’ liability under those laws will be limited at its option, to the supply of the Services again, or payment of the cost of having the Services supplied again.

Section 9.1(b) (Unlimited Liabilities) is replaced with the following:

b. Each party’s total aggregate Liability for damages arising out of or relating to the Agreement is limited to the greater of: (a) Fees Customer paid under the Order Form, and (b) AUD\$1,000.

Section 11.11 (Governing Law) is amended by inserting the following text at the end of that Section: “If applicable law prevents a dispute from being resolved in a California court, then Customer may file the dispute in Customer’s local courts. If applicable law prevents Customer’s local court from applying California law to resolve a dispute, then the dispute will be governed by the applicable local laws of Customer’s country, state, or other place of residence.”

Section 11.15 (Entire Agreement) is amended by inserting the following text at the end of that Section: “Nothing in this Agreement excludes a party’s liability for prior written or oral misrepresentation.”

Europe, Middle East, Africa

Europe, the Middle East, and Africa

1. Section 3.2 (Taxes) is replaced with:

Taxes. Google will itemise any invoiced Taxes. Customer will pay invoiced amounts without any deduction or withholding.

2. Section 3.4 (Overdue Payments) is replaced with:

Overdue Payments.

a. Customer's payment of Fees is overdue if Google has not received it by the Payment Due Date. If Customer's payment is overdue, Google may: (i) charge interest on overdue amounts at 2% per year above the base rate of Barclays Bank PLC from the Payment Due Date until paid in full whether before or after judgment, and (ii) Suspend the Services or terminate the applicable Order Form.

b. Customer will reimburse Google for all reasonable expenses (including legal fees) incurred by Google in collecting overdue payments except where such payments are due to Google's billing inaccuracies.

3. Section 6.4 (Disclaimer) is replaced with:

Disclaimer. No conditions, warranties or other terms apply to the provision of the Services or Deliverables unless expressly described in the Agreement. No implied conditions, warranties or other terms apply (including any implied terms as to satisfactory quality, fitness for purpose or conformance with description). Google does not warrant that operation of the Services or Deliverables will be error-free or uninterrupted.

4. Section 7.3(b) (Termination of the Agreement) is replaced with:

Termination of the Agreement. Either party may terminate the Agreement if the other party: (i) is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written notice; or (ii) enters into an arrangement or composition with or for the benefit of its creditors, goes into administration, receivership or administrative receivership, or is dissolved or otherwise ceases its business operations or becomes subject to insolvency or bankruptcy proceedings and such proceedings are not dismissed within 90 days.

5. Section 8.1 (Google Indemnification Obligations) is replaced with:

Google Indemnification Obligations. Google will indemnify Customer and its Affiliates participating under the Agreement ("Customer Indemnified Parties"), against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that Customer Indemnified Parties' use in accordance with the Agreement of Google Indemnified Materials infringes the third party's Intellectual Property Rights.

6. Section 8.2 (Customer Indemnification Obligations) is replaced with:

Customer Indemnification Obligations. Customer will indemnify Google, its Personnel, and its Affiliates, against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from any Customer Indemnified Materials.

7. Section 9 (Liability) is replaced with:

Liability.

9.1 *Limited Liabilities.*

a. Subject to Section 9.2 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Agreement for any:

- i. loss of profits;
- ii. loss of anticipated savings;
- iii. loss of business opportunity;
- iv. loss of reputation or goodwill; or
- v. indirect or consequential losses.

b. Subject to Sections 9.1(a) and 9.2 (Unlimited Liabilities), each party's total Liability for all claims arising out of or relating to the Agreement in any Contract Year is limited to the greater of:

- i. the total Fees paid by Customer in the relevant Contract Year for the Services (if any); and
- ii. £25,000.

9.2 Unlimited Liabilities. Nothing in the Agreement excludes or limits either party's Liability for:

- i. death or personal injury resulting from its negligence or the negligence of its employees or agents;
- ii. its fraud or fraudulent misrepresentation;
- iii. its infringement of the other party's Intellectual Property Rights;
- iv. its payment obligations under the Agreement;
- v. or matters for which liability cannot be excluded or limited under applicable law.

8. Section 11.11 (Governing Law) is replaced with:

Governing Law.

a. The Agreement and any dispute (contractual or non-contractual) concerning the Agreement or its subject matter or formation (a "Dispute") is/are governed by English law.

b. Any Dispute will be referred to and finally resolved by arbitration under the rules of the LCIA, which rules are deemed to be incorporated by reference into this Section. The number of arbitrators will be three. The seat, or legal place, of arbitration will be London, England. The language to be used in the arbitration will be English.

c. This Section 11.11 is without prejudice to the right of either party to apply to any court of competent jurisdiction for emergency, interim or injunctive relief (together "Interim Relief"). Except where Customer has its registered office or

principal place of business in Russia or Ukraine, such Interim Relief will be subject to review and subsequent adjudication by the arbitral tribunal such that any dispute in respect of Interim Relief will be determined by the arbitral tribunal.

9. The following new Definitions are added to Section 12:

“*commercially reasonable efforts*” means reasonable endeavours.

“*Contract Year*” means a period of one calendar year starting on the Effective Date or the relevant anniversary of the Effective Date (as appropriate).

10. The Definition below is replaced with the following language:

“*Tax(es)*” means any duties, customs fees, or taxes (other than Google’s income tax), including indirect taxes such as goods and services tax and value-added tax, associated with the purchase of the Services, and any related penalties or interest.

Previous versions (*Last modified September 11, 2025*)

January 30 2025, October 16 2024, November 16 2023, April 19 2023, December 16 2020, May 11 2020, March 26 2020, February 12 2020, January 31 2020, November 21 2019, October 1 2019, May 30 2019

Cloud Data Processing Addendum (Customers)

For translations of this Cloud Data Processing Addendum into other languages, please click on the appropriate link: Bahasa Indonesia (<https://services.google.com/fh/files/misc/id-cloud-data-processing-addendum-customers.pdf>), Deutsch (<https://services.google.com/fh/files/misc/de-cloud-data-processing-addendum-customers.pdf>), Español (Latinoamérica) (<https://services.google.com/fh/files/misc/es-419-cloud-data-processing-addendum-customers.pdf>), Français (<https://services.google.com/fh/files/misc/fr-cloud-data-processing-addendum-customers.pdf>), Italiano (<https://services.google.com/fh/files/misc/it-cloud-data-processing-addendum-customers.pdf>), Nederlands (<https://services.google.com/fh/files/misc/nl-cloud-data-processing-addendum-customers.pdf>), Português (<https://services.google.com/fh/files/misc/pt-br-cloud-data-processing-addendum-customers.pdf>), 한국어 (<https://services.google.com/fh/files/misc/ko-cloud-data-processing-addendum-customers.pdf>), 日本語 (<https://services.google.com/fh/files/misc/ja-cloud-data-processing-addendum-customers.pdf>)

This Cloud Data Processing Addendum (including its appendices, the “Addendum”) is incorporated into the Agreement(s) (as defined below) between Google and Customer. This Addendum was formerly known as the “Data Processing and Security Terms” under an Agreement for Google Cloud Platform, Looker (original), Google SecOps Services, or Google Skills for Organizations; the “Data Processing Amendment” under an Agreement for Google Workspace or Cloud Identity; and the “Data Processing Addendum” under an Agreement for Mandiant Consulting Services and Managed Services.

General Terms

1. Overview

This Addendum describes the parties’ obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer Data (as defined below). This Addendum will be effective on the Addendum Effective Date (as defined below), and will replace any terms previously applicable to the processing and security of Customer Data. Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement.

2. Definitions

2.1 In this Addendum:

- “*Addendum Effective Date*” means the date on which Customer accepted, or the parties otherwise agreed to, this Addendum.
- “*Additional Security Controls*” means security resources, features, functionality, and controls that Customer may use at its option and as it determines, including the Admin Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- “*Agreement*” means the contract under which Google has agreed to provide the applicable Services to Customer.
- “*Applicable Privacy Law*” means, as applicable to the processing of Customer Personal Data, any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation. For clarity, Applicable Privacy Laws include but are not limited to the laws mentioned in Appendix 3 (Specific Privacy Laws).
- “*Audited Services*” means the then-current Services indicated as being in-scope for the relevant certification or report at <https://cloud.google.com/security/compliance/services-in-scope>. Google may not remove any Services from this URL unless they have been discontinued in accordance with the applicable Agreement.
- “*Compliance Certifications*” has the meaning given in Section 7.4 (Compliance Certifications and SOC Reports).
- “*Customer Data*”, if not defined in the Agreement, has the meaning given in Appendix 4 (Specific Products).
- “*Customer Personal Data*” means the personal data contained within the Customer Data, including any special categories of personal data or sensitive data defined under Applicable Privacy Law.
- “*Data Incident*” means a breach of Google’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google.
- “*EMEA*” means Europe, the Middle East and Africa.
- “*EU GDPR*” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- “*European Data Protection Law*” means, as applicable: (a) the GDPR; or (b) the Swiss FADP.
- “*European Law*” means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data); or (c) the law of Switzerland (if the Swiss FADP applies to the processing of Customer Personal Data).
- “*GDPR*” means, as applicable: (a) the EU GDPR; or (b) the UK GDPR.
- “*Google’s Third-Party Auditor*” means a Google-appointed, qualified and independent third-party auditor, whose then-current identity Google will disclose to Customer.
- “*Instructions*” has the meaning given in Section 5.2 (Compliance with Customer’s Instructions).

- “*Notification Email Address*” means the email address(es) designated by Customer in the Admin Console or Order Form to receive certain notifications from Google.
- “*Security Documentation*” means the Compliance Certifications and the SOC Reports.
- “*Security Measures*” has the meaning given in Section 7.1.1 (Google’s Security Measures).
- “*Services*” means the applicable services described in Appendix 4 (Specific Products).
- “*SOC Reports*” has the meaning given in Section 7.4 (Compliance Certifications and SOC Reports).
- “*Subprocessor*” means a third party authorized as another processor under this Addendum to process Customer Data in order to provide parts of the Services and TSS (if applicable).
- “*Supervisory Authority*” means, as applicable: (a) a “supervisory authority” as defined in the EU GDPR; or (b) the “Commissioner” as defined in the UK GDPR or the Swiss FADP.
- “*Swiss FADP*” means, as applicable, the Federal Act on Data Protection of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 14 June 1993) or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022).
- “*Term*” means the period from the Addendum Effective Date until the end of Google’s provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Google may continue providing the Services for transitional purposes.
- “*UK GDPR*” means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

2.2 The terms “personal data”, “data subject”, “processing”, “controller”, and “processor” as used in this Addendum have the meanings given by Applicable Privacy Law or, absent any such meaning or law, by the EU GDPR.

2.3 The terms “data subject”, “controller” and “processor” include “consumer”, “business”, and “service provider”, respectively, as required by Applicable Privacy Law.

3. Duration

Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Google deletes all Customer Data as described in this Addendum.

4. Roles; Legal Compliance

4.1 *Roles of Parties.* Google is a processor and Customer is a controller or processor, as applicable, of Customer Personal Data.

4.2 Processing Summary. The subject matter and details of the processing of Customer Personal Data are described in Appendix 1 (Subject Matter and Details of Data Processing).

4.3 Compliance with Law. Each party will comply with its obligations related to the processing of Customer Personal Data under Applicable Privacy Law.

4.4 Additional Legal Terms. To the extent the processing of Customer Personal Data is subject to an Applicable Privacy Law described in Appendix 3 (Specific Privacy Laws), the corresponding terms in Appendix 3 will apply in addition to these General Terms and prevail as described in Section 14.1 (Precedence).

5. Data Processing

5.1 Processor Customers. If Customer is a processor:

a. Customer warrants on an ongoing basis that the relevant third-party controller has authorized:

- i. the Instructions;
- ii. Customer's engagement of Google as another processor; and
- iii. Google's engagement of Subprocessors as described in Section 11 (Subprocessors);

b. Customer will forward to the third-party controller promptly and without undue delay any notice provided by Google under Section 7.2.1 (Incident Notification), 9.2.1 (Responsibility for Requests), or 11.4 (Opportunity to Object to Subprocessors); and

c. Customer may make available to the third-party controller any other information made available by Google under this Addendum about the locations of Google data centers or the names, locations and activities of Subprocessors.

5.2 Compliance with Customer's Instructions. Customer instructs Google to process Customer Data in accordance with the applicable Agreement (including this Addendum) only as follows:

a. to provide, secure, and monitor the Services and TSS (if applicable); and

b. as further specified via:

- i. Customer's use of the Services (including via the Admin Console) and TSS (if applicable); and
- ii. any other written instructions given by Customer and acknowledged by Google as constituting instructions under this Addendum (collectively, the "*Instructions*").

Google will comply with the Instructions unless prohibited by European Law, where European Data Protection Law applies, or prohibited by applicable law, where any other Applicable Privacy Law applies.

6. Data Deletion

6.1 Deletion by Customer. Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Google to delete the relevant Customer Data from Google's systems. Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

6.2 Return or Deletion When Term Ends. If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google in accordance with Section 9.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 6.3 (Deferred Deletion Instruction), Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google's systems at the end of the Term. After a recovery period of up to 30 days from that date, Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

6.3. Deferred Deletion Instruction. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Return or Deletion When Term Ends) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will take effect with respect to such Customer Data only when the continuing Term expires. For clarity, this Addendum will continue to apply to such Customer Data until its deletion by Google.

7. Data Security

7.1 Google's Security Measures, Controls and Assistance.

7.1.1 Google's Security Measures. Google will implement and maintain technical, organizational, and physical measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (Security Measures) (the "**Security Measures**"). The Security Measures include measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.

7.1.2 Access and Compliance. Google will:

- a. authorize its employees, contractors and Subprocessors to access Customer Data only as strictly necessary to comply with Instructions;
- b. take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance; and
- c. ensure that all persons authorized to process Customer Data are under an obligation of confidentiality.

7.1.3 Additional Security Controls. Google will make Additional Security Controls available to:

- a. allow Customer to take steps to secure Customer Data; and
- b. provide Customer with information about securing, accessing and using Customer Data.

7.1.4 Google's Security Assistance. Google will (taking into account the nature of the processing of Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with its (or, where Customer is a processor, the third-party controller's) obligations relating to security and personal data breaches under Applicable Privacy Law, by:

- a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);
- b. making Additional Security Controls available in accordance with Section 7.1.3 (Additional Security Controls);
- c. complying with the terms of Section 7.2 (Data Incidents);
- d. making the Security Documentation available in accordance with Section 7.5.1 (Reviews of Security Documentation) and providing the information contained in the applicable Agreement (including this Addendum); and
- e. if subsections (a)-(d) above are insufficient for Customer (or the third-party controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

7.2 Data Incidents.

7.2.1 Incident Notification. Google will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Details of Data Incident. Google's notification of a Data Incident will describe: the nature of the Data Incident including the Customer resources impacted; the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Google recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Google's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2.3 No Assessment of Customer Data by Google. Google has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

7.2.4 No Acknowledgement of Fault by Google. Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

7.3 Customer's Security Responsibilities and Assessment.

7.3.1 Customer's Security Responsibilities. Without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the applicable Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Google's or Google's Subprocessors' systems, including:

- a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk to the Customer Data;
- b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and
- c. backing up or retaining copies of its Customer Data as appropriate.

7.3.2 Customer's Security Assessment. Customer agrees that the Services, Security Measures, Additional Security Controls, and Google's commitments under this Section 7 (Data Security) provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Data as well as the risks to individuals).

7.4 Compliance Certifications and SOC Reports. Google will maintain at least the following for the Audited Services to verify the continued effectiveness of the Security Measures:

- a. certificates for ISO 27001 and any additional certifications described in Appendix 4 (Specific Products) (the “*Compliance Certifications*”); and
- b. SOC 2 and SOC 3 reports produced by Google’s Third-Party Auditor and updated annually based on an audit performed at least once every 12 months (the “*SOC Reports*”).

Google may add standards at any time. Google may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

7.5 Reviews and Audits of Compliance.

7.5.1 Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the Security Documentation available for review by Customer and, if Customer is a processor, allow Customer to request access to the SOC Reports for the third-party controller in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

7.5.2 Customer’s Audit Rights.

- a. *Customer Audit.* Google will, if required under Applicable Privacy Law, allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google’s compliance with its obligations under this Addendum in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). During an audit, Google will reasonably cooperate with Customer or its auditor as described in this Section 7.5 (Reviews and Audits of Compliance).
- b. *Customer Independent Review.* Customer may conduct an audit to verify Google’s compliance with its obligations under this Addendum by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google’s Third-Party Auditor).

7.5.3 Additional Business Terms for Reviews and Audits.

- a. Customer must contact Google’s Cloud Data Protection Team to request:
 - i. access to the SOC Reports for a third-party controller under Section 7.5.1 (Reviews of Security Documentation); or
 - ii. an audit under Section 7.5.2(a) (Customer Audit).
- b. Following a Customer request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on:
 - i. security and confidentiality controls applicable to any access to the SOC Reports by a third-party controller under Section 7.5.1 (Reviews of Security Documentation); and
 - ii. the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) (Customer Audit).
- c. Google may charge a fee (based on Google’s reasonable costs) for any audit under Section 7.5.2(a) (Customer Audit). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.
- d. Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) (Customer Audit) if the auditor is, in Google’s reasonable opinion, not suitably qualified or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection by Google will require Customer to appoint another auditor or conduct the audit itself.
- e. Any Customer requests under Appendix 3 (Specific Privacy Laws) or Appendix 4 (Specific Products) for access to any SOC reports for a third-party controller or for

audits will also be subject to this Section 7.5.3 (Additional Business Terms for Reviews and Audits).

8. Impact Assessments and Consultations

Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with its (or, where Customer is a processor, the third-party controller's) obligations relating to data protection assessments, risk assessments, prior regulatory consultations or equivalent procedures under Applicable Privacy Law, by:

- a. making Additional Security Controls available in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation available in accordance with Section 7.5.1 (Reviews of Security Documentation);
- b. providing the information contained in the applicable Agreement (including this Addendum); and
- c. if subsections (a) and (b) above are insufficient for Customer (or the third-party controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

9. Access; Data Subject Rights; Data Export

9.1 Access; Rectification; Restricted Processing; Portability. During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by Applicable Privacy Law.

9.2 Data Subject Requests.

9.2.1 Responsibility for Requests. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will:

- a. advise the data subject to submit their request to Customer;
- b. promptly notify Customer; and
- c. not otherwise respond to that data subject's request without authorization from Customer.

Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 Google's Data Subject Request Assistance. Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the third-party controller's) obligations under Applicable Privacy Law to respond to requests for exercising the data subject's rights by:

- a. making Additional Security Controls available in accordance with Section 7.1.3 (Additional Security Controls);
- b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and
- c. if subsections (a) and (b) above are insufficient for Customer (or the third-party controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

10. Data Processing Locations

10.1 *Data Storage and Processing Facilities.* Subject to Google's data location commitments under the Service Specific Terms and data transfer commitments under Appendix 3 (Specific Privacy Laws), if applicable, Customer Data may be processed in any country where Google or its Subprocessors maintain facilities.

10.2 *Data Center Information.* The locations of Google data centers are described in Appendix 4 (Specific Products).

11. Subprocessors

11.1 *Consent to Subprocessor Engagement.* Customer specifically authorizes Google's engagement as Subprocessors of those entities disclosed as described in Section 11.2 (Information about Subprocessors) as of the Addendum Effective Date. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessors), Customer generally authorizes Google's engagement of other third parties as Subprocessors ("New Subprocessors").

11.2 *Information about Subprocessors.* Names, locations, and activities of Subprocessors are described in Appendix 4 (Specific Products).

11.3 *Requirements for Subprocessor Engagement.* When engaging any Subprocessor, Google will:

a. ensure via a written contract that:

- i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Addendum); and
- ii. if required under Applicable Privacy Laws, the data protection obligations described in this Addendum are imposed on the Subprocessor (as may be further described in Appendix 3 (Specific Privacy Laws)); and

b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 *Opportunity to Object to Subprocessors.*

a. When Google engages any New Subprocessor during the Term, Google will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name, location and activities of the New Subprocessor).

b. Customer may, within 90 days after being notified of the engagement of a New Subprocessor, object by immediately terminating the applicable Agreement for convenience:

- i. in accordance with that Agreement's termination for convenience provision; or
- ii. if there is no such provision, by notifying Google.

12. Cloud Data Protection Team; Processing Records

12.1 *Cloud Data Protection Team.* Google's Cloud Data Protection Team will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Data under the applicable Agreement and can be contacted as described in the Notices section of the applicable Agreement or in Appendix 4 (Specific Products).

12.2 *Google's Processing Records.* Google will keep appropriate documentation of its processing activities as required by Applicable Privacy Law. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will use the Admin Console or other

means identified in Appendix 4 (Specific Products) to supply such information and keep it accurate and up-to-date. Google may make any such information available to competent regulators, including a Supervisory Authority, if required by Applicable Privacy Law.

12.3 Controller Requests. During the Term, if Google's Cloud Data Protection Team receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Google will advise the third party to contact Customer.

13. Notices

Notices under this Addendum (including notifications of any Data Incidents) will be delivered to the Notification Email Address. Customer is responsible for using the Admin Console, or otherwise notifying Google, to ensure that its Notification Email Address remains current and valid.

14. Interpretation

14.1 Precedence. To the extent of any conflict between:

- a. Appendix 3 (Specific Privacy Laws) and the remainder of the Addendum (including Appendix 4 (Specific Products)), Appendix 3 will prevail; and
 - b. Appendix 4 (Specific Products) and the remainder of the Addendum (excluding Appendix 3), Appendix 4 will prevail; and
 - c. this Addendum and the remainder of the Agreement, this Addendum will prevail.
- For clarity, if Customer has more than one Agreement, this Addendum will amend each of the Agreements separately.

14.2 Section References. Unless indicated otherwise, section references in any Appendix to this Addendum refer to sections of the General Terms of the Addendum.

Appendix 1: Subject Matter and Details of Data Processing

Subject Matter

Google's provision of the Services and TSS (if applicable) to Customer.

Duration of the Processing

The Term plus the period from the end of the Term until deletion of all Customer Data by Google in accordance with this Addendum.

Nature and Purpose of the Processing

Google will process Customer Personal Data for the purposes of providing the Services and TSS (if applicable) to Customer in accordance with this Addendum.

Categories of Data

Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer or by its End Users.

Data Subjects

Data subjects include the individuals about whom data is provided to Google via the Services by (or at the direction of) Customer or by its End Users.

Appendix 2: Security Measures

As from the Addendum Effective Date, Google will implement and maintain the Security Measures described in this Appendix 2.

1. Data Center and Network Security

(a) Data Centers.

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy.

Code Quality. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks and Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves: (i) tightly controlling the size and make-up of Google's attack surface through preventative measures; (ii) employing intelligent detection controls at data entry points; and (iii) employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls

(a) Site Controls.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ a dual authentication access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing

monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and systems from gaining access to systems used to process Customer Data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Google's authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g. credit card data), Google uses hardware tokens.

3. Data

(a) *Data Storage, Isolation and Logging.* Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data. Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.

(b) *Decommissioned Disks and Disk Erase Policy.* Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial

number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Google personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g. certifications). Google's personnel will not process Customer Data without authorization.

5. Subprocessor Security

Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Appendix 3: Specific Privacy Laws

The terms in each subsection of this Appendix 3 apply only where the corresponding law applies to the processing of Customer Personal Data.

European Data Protection Law

1. Additional Definitions.

- *"Adequate Country"* means:

(a) for data processed subject to the EU GDPR: the European Economic Area, or a country or territory recognized as ensuring adequate protection under the EU GDPR;

(b) for data processed subject to the UK GDPR: the UK, or a country or territory recognized as ensuring adequate protection under the UK GDPR and the Data Protection Act 2018; or

(c) for data processed subject to the Swiss FADP: Switzerland, or a country or territory that is: (i) included in the list of the states whose legislation ensures adequate protection as published by the Swiss Federal Data Protection and Information Commissioner, if applicable; or (ii) recognized as ensuring adequate protection by the Swiss Federal Council under the Swiss FADP;

in each case, other than on the basis of an optional data protection framework.

- *"Alternative Transfer Solution"* means, for purposes of these European Data Protection Law terms, a solution, other than SCCs, that enables the lawful

transfer of personal data to a third country in accordance with European Data Protection Law, for example a data protection framework recognized as ensuring that participating entities provide adequate protection.

- “*Customer SCCs*” means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Processor), or the SCCs (Processor-to-Controller), as applicable.
- “*SCCs*” means the Customer SCCs or SCCs (Processor-to-Processor, Google Exporter), as applicable.
- “*SCCs (Controller-to-Processor)*” means the terms at <https://cloud.google.com/terms/sccs/eu-c2p>.
- “*SCCs (Processor-to-Controller)*” means the terms at <https://cloud.google.com/terms/sccs/eu-p2c>.
- “*SCCs (Processor-to-Processor)*” means the terms at <https://cloud.google.com/terms/sccs/eu-p2p>.
- “*SCCs (Processor-to-Processor, Google Exporter)*” means the terms at <https://cloud.google.com/terms/sccs/eu-p2p-google-exporter>.

2. Instruction Notifications. Without prejudice to Google’s obligations under Section 5.2 (Compliance with Customer’s Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will immediately notify Customer if, in Google’s opinion:

- a. European Law prohibits Google from complying with an Instruction;
 - b. an Instruction does not comply with European Data Protection Law; or
 - c. Google is otherwise unable to comply with an Instruction,
- in each case unless such notice is prohibited by European Law.

If Customer is a processor, Customer will immediately forward to the third-party controller any notice provided by Google under this section.

3. Customer’s Audit Rights. Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) as described in Section 7.5.2(a) (Customer Audit). During such an audit, Google will make available all information necessary to demonstrate compliance with its obligations under this Addendum and contribute to the audit as described in Section 7.5 (Reviews and Audits of Compliance) and this section.

4. Data Transfers.

4.1 Restricted Transfers. The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and European Data Protection Law applies to the transfers (as certified by Customer under Section 4.2 (Certification by Non-EMEA Customers) of these European Data Protection Law terms, if its billing address is outside EMEA) (“*Restricted Transfers*”), then:

- a. if Google has adopted an Alternative Transfer Solution for any Restricted Transfers, Google will inform Customer of the relevant solution and ensure that such Restricted Transfers are made in accordance with it; or
- b. if Google has not adopted an Alternative Transfer Solution for any Restricted Transfers, or informs Customer that Google is no longer adopting, an Alternative

Transfer Solution for any Restricted Transfers (without adopting a replacement Alternative Transfer Solution):

i. if Google's address is in an Adequate Country:

A. the SCCs (Processor-to-Processor, Google Exporter) will apply with respect to such Restricted Transfers from Google to Subprocessors; and

B. in addition, if Customer's billing address is not in an Adequate Country, the SCCs (Processor-to Controller) will apply (regardless of whether Customer is a controller or processor) with respect to such Restricted Transfers between Google and Customer; or

ii. if Google's address is not in an Adequate Country, the SCCs (Controller-to-Processor) or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller or processor) with respect to such Restricted Transfers between Google and Customer.

4.2 Certification by Non-EMEA Customers. If Customer's billing address is outside EMEA, and the processing of Customer Personal Data is subject to European Data Protection Law, then unless Appendix 4 (Specific Products) of this Addendum indicates otherwise, Customer will certify as such and identify its competent Supervisory Authority via the Admin Console for the applicable Services.

4.3 Information about Restricted Transfers. Google will provide Customer with information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures:

a. as described in Section 7.5.1 (Reviews of Security Documentation);

b. in any additional locations described in Appendix 4 (Specific Products); and

c. in relation to Google's adoption of an Alternative Transfer Solution, at <https://cloud.google.com/terms/alternative-transfer-solution>.

4.4 SCC Audits. If Customer SCCs apply as described in Section 4.1 (Restricted Transfers) of these European Data Protection Law terms, Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

4.5 SCCs and Third-Party Controllers. If Customer is a processor, Customer acknowledges that Google, as another processor, may not be able to identify the third-party controller and, accordingly, Customer will forward to the third-party controller promptly and without undue delay any notice that refers to any SCCs.

4.6 Termination Due to Data Transfer Risk. If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable Agreement in accordance with that Agreement's termination for convenience provision or, if there is no such provision, by notifying Google.

4.7 No Modification of SCCs. Nothing in the Agreement (including this Addendum) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

4.8 Precedence of SCCs. To the extent of any conflict or inconsistency between any Customer SCCs (which are incorporated by reference into this Addendum) and the remainder of the Agreement (including this Addendum), the Customer SCCs will prevail.

5. Requirements for Subprocessor Engagement. European Data Protection Law requires Google to ensure via a written contract that the data protection obligations described in this Addendum, as referred to in Article 28(3) of the GDPR, if applicable, are imposed on any Subprocessor engaged by Google.

CCPA

1. Additional Definitions.

- “*CCPA*” means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.
- “*Customer Personal Data*” includes “personal information”.
- The terms “business”, “business purpose”, “consumer”, “personal information”, “processing”, “sale”, “sell”, “service provider”, and “share” have the meanings given in the CCPA.

2. Prohibitions. Without prejudice to Google’s obligations under Section 5.2 (Compliance with Customer’s Instructions), with respect to the processing of Customer Personal Data in accordance with the CCPA, Google will not, unless otherwise permitted under the CCPA:

- a. sell or share Customer Personal Data;
- b. retain, use or disclose Customer Personal Data:
 - i. other than for a business purpose under the CCPA on behalf of Customer and for the specific purpose of performing the Services and TSS (if applicable); or
 - ii. outside of the direct business relationship between Google and Customer; or
- c. combine or update Customer Personal Data with personal information that Google receives from or on behalf of a third party or collects from its own interactions with the consumer.

3. Compliance. Without prejudice to Google’s obligations under Section 5.2 (Compliance with Customer’s Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will notify Customer if, in Google’s opinion, Google is unable to meet its obligations under the CCPA, unless such notice is prohibited by applicable law.

4. Customer Intervention. If Google notifies Customer of any unauthorized use of Customer Personal Data, including under Section 3 (Compliance) of this subsection or Section 7.2.1 (Incident Notification), Customer may take reasonable and appropriate steps to stop or remediate such unauthorized use by:

- a. taking any measures recommended by Google pursuant to Section 7.2.2 (Details of Data Incident), if applicable; or
- b. exercising its rights under Section 7.5.2(a) (Customer Audit) or 9.1 (Access; Rectification; Restricted Processing; Portability).

Turkey

1. Additional Definitions.

- “*Turkish Data Protection Law*” means the Turkish Law on the Protection of Personal Data No. 6698 dated April 7, 2016.

- “*Turkish Personal Data Protection Authority*” means the Kişisel Verileri Koruma Kurumu.
- “*Turkish SCCs*” means standard contract clauses under Turkish Data Protection Law.

2. Data Transfers.

2.1 *Supplementary Terms.* If Customer’s billing address is in Turkey and Google makes any optional additional terms (including Turkish SCCs) available for acceptance by Customer in relation to transfers of Customer Personal Data under Turkish Data Protection Law, those terms will supplement this Addendum as from the date they are notified to the Turkish Personal Data Protection Authority in accordance with Section 2.2 (Notification to the Competent Authority) below, as evidenced by Customer to Google.

2.2 *Notification to the Competent Authority.* If Customer enters into Turkish SCCs under this Section 2 (Data Transfers), Customer will be responsible for notifying the Turkish Personal Data Protection Authority of use of Turkish SCCs within five (5) business days of signature of the Turkish SCCs as required by Turkish Data Protection Law.

2.3 *SCC Audits.* If Customer enters into Turkish SCCs under this Section 2 (Data Transfers), Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

2.4 *Termination Due to Data Transfer Risk.* If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable Agreement in accordance with that Agreement’s termination for convenience provision or, if there is no such provision, by notifying Google.

2.5 *No Modification of Turkish SCCs.* Nothing in the Agreement (including this Addendum) is intended to modify or contradict the Turkish SCCs or prejudice the fundamental rights or freedoms of data subjects under Turkish Data Protection Law.

2.6 *Precedence of SCCs.* To the extent of any conflict or inconsistency between the Turkish SCCs (which will be incorporated by reference into this Addendum if entered into by Customer) and the remainder of the Agreement (including this Addendum), the Turkish SCCs will prevail.

Israel

1. Additional Definition.

- “*Israeli Privacy Protection Law*” means the Israeli Privacy Protection Law, 1981 and any regulations promulgated thereunder.

2. *Equivalent Terms.* Any terms equivalent to “controller”, “personal data”, “processing”, and “processor”, as used in this Addendum, have the meanings given in the Israeli Privacy Protection Law.

3. *Customer’s Audit Rights.* Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) as described in Section 7.5.2(a) (Customer Audit).

Brazil

1. Additional Definitions.

- “*Adequate Country*” means, for data processed subject to the LGPD, Brazil or a country or international organization recognized by the Brazilian Data Protection Authority (ANPD, in the Portuguese acronym) as ensuring adequate protection under the LGPD.
- “*Alternative Transfer Solution*” means, for purposes of these Brazilian terms, a solution, other than the BR SCCs, that enables the lawful international transfer of personal data in accordance with the LGPD.
- “*BR SCCs*” means the BR SCCs (Controller-to-Processor), the BR SCCs (Processor-to-Processor) or BR SCCs (Processor-to-Processor, Google Exporter), as applicable.
- “*BR SCCs (Controller-to-Processor)*” means the terms at <https://cloud.google.com/sccs/br-c2p?hl=pt-br>.
- “*BR SCCs (Processor-to-Processor)*” means the terms at <https://cloud.google.com/sccs/br-p2p?hl=pt-br>.
- “*BR SCCs (Processor-to-Processor, Google Exporter)*” means the terms at <https://cloud.google.com/sccs/br-p2p-intra-group?hl=pt-br>.
- “*LGPD*” means the Brazilian Law No. 13,709/2018, as amended.

2. Instruction Notifications. Without prejudice to Google’s obligations under Section 5.2 (Compliance with Customer’s Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will immediately notify Customer if, in Google’s opinion:

- a. Brazilian law prohibits Google from complying with an Instruction;
 - b. an Instruction does not comply with the LGPD; or
 - c. Google is otherwise unable to comply with an Instruction,
- in each case unless such notice is prohibited by Brazilian law.

If Customer is a processor, Customer will immediately forward to the third-party controller any notice provided by Google under this section.

3. Data Transfers.

3.1. Restricted Transfers. The parties acknowledge that the LGPD does not require BR SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and the LGPD applies to the transfers (“*BR Restricted Transfers*”), then:

- a. if Google has adopted an Alternative Transfer Solution for any BR Restricted Transfers, Google will inform Customer of the relevant solution and ensure that such Restricted Transfers are made in accordance with it; or
- b. if Google has not adopted an Alternative Transfer Solution for any BR Restricted Transfers, or informs Customer that Google is no longer adopting, an Alternative Transfer Solution for any BR Restricted Transfers (without adopting a replacement Alternative Transfer Solution):
 - i. if Google’s address is in an Adequate Country, the BR SCCs (Processor-to-Processor, Google Exporter) will apply with respect to such Restricted Transfers from Google to Subprocessors; or
 - ii. if Google’s address is not in an Adequate Country, the BR SCCs (Controller-to-Processor) or BR SCCs (Processor-to-Processor) will apply (according

to whether Customer is a controller or processor) with respect to such Restricted Transfers between Google and Customer.

3.2. *Information about Restricted Transfers.* Google will provide Customer with information relevant to BR Restricted Transfers, Additional Security Controls and other supplementary protective measures:

- a. as described in Section 7.5.1 (Reviews of Security Documentation);
- b. in any additional locations described in Appendix 4 (Specific Products); and
- c. in relation to Google's adoption of an Alternative Transfer Solution, at <https://cloud.google.com/terms/alternative-transfer-solution>.

3.3. *SCCs and Third-Party Controllers.* If Customer is a processor, Customer acknowledges that Google, as another processor, may not be able to identify the third-party controller and, accordingly, Customer will:

- a. forward to the third-party controller promptly and without undue delay any notice that refers to any BR SCCs;
- b. be solely responsible, as between Google and Customer, for ensuring the third-party controller's compliance with the transparency obligations under the BR SCCs; and
- c. upon Google's written request, promptly provide the following information regarding the third-party controller: name, corporate details (e.g. type of entity, registered address, tax identifier), main address, email address, data subject contact point and any details required by the BR SCCs in relation to Customer's contract with the controller.

3.4. *Termination Due to Data Transfer Risk.* If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable Agreement in accordance with that Agreement's termination for convenience provision or, if there is no such provision, by notifying Google.

3.5. *No Modification of SCCs.* Nothing in the Agreement (including this Addendum) is intended to modify or contradict the BR SCCs.

3.6. *Precedence of SCCs.* To the extent of any conflict or inconsistency between the BR SCCs (Controller-to-Processor) and BR SCCs (Processor-to-Processor) (which are incorporated as annexes into this Addendum as applicable) and the remainder of the Agreement (including this Addendum), the applicable SCCs will prevail.

Appendix 4: Specific Products

The terms in each subsection of this Appendix 4 apply solely with respect to the processing of Customer Data by the corresponding Service(s).

Google Cloud Platform

1. Additional Definitions.

- “*Account*”, if not defined in the Agreement, means Customer's Google Cloud Platform account.
- “*Customer Data*”, if not defined in the Agreement, means data provided to Google by Customer or End Users through Google Cloud Platform under the Account, and data that Customer or End Users derive from that data through their use of Google Cloud Platform.

- “*Google Cloud Platform*” means the Google Cloud Platform services described at <https://cloud.google.com/terms/services>, excluding any Third-Party Offerings.
- “*Third-Party Offerings*”, if not defined in the Agreement, means (a) third-party services, software, products, and other offerings that are not incorporated into Google Cloud Platform or Software, (b) offerings identified in the “Third-Party Terms” section of the Service Specific Terms of the Agreement, and (c) third-party operating systems.

2. Compliance Certifications. The Compliance Certifications for Google Cloud Platform Audited Services will also include certificates for ISO 27017 and ISO 27018 and a PCI DSS Attestation of Compliance.

3. Data Center Locations. The locations of Google Cloud Platform data centers are described at <https://cloud.google.com/about/locations/>.

4. Information about Subprocessors. Names, locations, and activities of Google Cloud Platform Subprocessors are described at <https://cloud.google.com/terms/subprocessors>.

5. Cloud Data Protection Team. The Data Protection Team for Google Cloud Platform can be contacted at <https://support.google.com/cloud/contact/dpo>.

6. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures is available at cloud.google.com/privacy/.

7. Service Specific Terms.

Bare Metal Solution (Google Cloud Platform)

Bare Metal Solution provides non-virtualized access to underlying infrastructure resources and, by design, has certain distinct characteristics.

1. Amendments. This Addendum is amended as follows with respect to Bare Metal Solution:

- The definition of “Google’s Third-Party Auditor” is replaced with the following:
 - “*Google’s Third-Party Auditor*” means a qualified and independent third-party auditor appointed by Google or a Bare Metal Solution Subprocessor, whose then-current identity Google will disclose to Customer on request.
- The following terms are deleted:
 - From Section 7.1.1 (Google’s Security Measures), the phrase “Encrypt Customer Data”;
 - From Appendix 2 (Security Measures), the Section 1(a) subsections titled “Server Operating Systems” and “Business Continuity”;
 - From Appendix 2, the Section 1(b) subsections titled “External Attack Surface,” “Intrusion Detection,” and “Encryption Technologies”; and
 - From Appendix 2, the following sentences of Section 3(a):
 - Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Customer instructions to the contrary (for example, in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers.

2. Compliance Certifications and SOC Reports. Google or its Subprocessor will maintain at least the following (or an equivalent or enhanced alternative) for Bare Metal Solution to verify the continued effectiveness of the Security Measures:

- a certificate for ISO 27001 and a PCI DSS Attestation of Compliance (the “*BMS Compliance Certifications*”); and
- SOC 1 and SOC 2 reports updated annually based on an audit performed at least once every 12 months (the “*BMS SOC Reports*”).

3. Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the BMS Compliance Certifications and BMS SOC Reports available for review by Customer and, if Customer is a processor, allow Customer to request access for the third-party controller to the BMS SOC Reports in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

4. Customer Obligations. Without limiting Google's express obligations related to Bare Metal Solution, Customer will take reasonable steps to protect and maintain the security of Customer Data and any other content stored on or processed through Bare Metal Solution.

5. Disclaimer. Notwithstanding anything to the contrary in the Agreement (including this Addendum), Google is not responsible for any of the following in relation to Bare Metal Solution:

- non-physical security, such as access controls, encryption, firewalls, antivirus protection, threat detection, and security scanning;
- logging and monitoring;
- non-hardware maintenance or support;
- data backup, including any redundancy or high-availability configuration; or
- business continuity and disaster recovery policies or procedures.

Customer is solely responsible for securing (other than physical security of Bare Metal Solution servers), logging and monitoring, maintaining and supporting, and backing up any Operating Systems, Customer Data, software, and applications Customer uses with, uploads to, or hosts on Bare Metal Solution.

Cloud NGFW (Google Cloud Platform)

The edition of Cloud NGFW titled “Cloud NGFW Enterprise” (“CNE”) is designed to mitigate cybersecurity risks and, as such, has certain distinct characteristics.

1. Amendments. The Addendum is amended as follows with respect to CNE:

- Sections 6.1 (Deletion by Customer) and 6.2 (Return or Deletion When Term Ends) will not prevent Google or Subprocessors from retaining any file or network traffic packet capture submitted for TSS purposes and designated by CNE as a security threat, provided that the file or network traffic packet capture does not include Customer Personal Data.

Google Distributed Cloud connected (Google Cloud Platform)

Google Distributed Cloud connected is not deployed at a Google data center and, by design, has certain distinct characteristics.

1. Amendments. This Addendum is amended as follows with respect to Google Distributed Cloud connected:

- The definition of “Data Incident” is replaced with the following:
 - “*Data Incident*” means a breach of Google’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized

disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google, but for clarity excluding any breaches that are connected to hardware or infrastructure that is managed, hosted or operated by, or otherwise the responsibility of, Customer.

- References to “Google’s systems” are replaced with “the Equipment.”
- Section 6.2 (Return or Deletion When Term Ends) is replaced with the following:
 - **6.2 Return or Deletion at the end of the Term.** Customer instructs Google to delete all remaining Customer Data (including existing copies) from the Equipment at the end of the Term in accordance with applicable law. If Customer wishes to retain any Customer Data after the end of the Term, it may export or make copies of such data prior to the end of the Term. Google will comply with the Instruction in this Section 6.2 as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.
- The following words are added to the end of Section 10.1 (Data Storage and Processing Facilities): “or where the Customer Location is located.”
- Section 1 (Data Center and Network Security) of Appendix 2 (Security Measures) is replaced with the following:

- **1. Local Machines and Network Security**

Local Machines. Customer Data is solely stored on the Equipment to be deployed in a Customer Location.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Google employs a code review process to increase the security of the code used to provide Google Distributed Cloud connected and enhance the security products in Google Distributed Cloud connected production environments.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available and allows for encryption of data in transit. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough. Google also makes encryption of data at rest available, using at least AES128 or similar. Google Distributed Cloud connected has a CMK integration; more information can be found at <https://cloud.google.com/kms/docs/cmek>.

Connection to Cloud VPN. Google allows Customer to enable and configure a strong, encrypted interconnection between the Equipment and Customer’s Virtual Private Cloud using Cloud VPN through an IPSEC VPN connection.

Bound Storage. Customer’s data storage is bound to the server. Should a disk be stolen or copied at rest, the contents of such disk will be unrecoverable outside of the server.

- Sections 2 (Access and Site Controls) and 3 (Data) of Appendix 2 (Security Measures) are deleted.

2. Inapplicable Provisions. Any Google obligations in the Agreement (including this Addendum) or statements in associated security documentation (including

whitepapers) that depend on Google's operation of a Google data center do not apply to Google Distributed Cloud connected.

Google-Managed Multi-Cloud (Google Cloud Platform)

Google-Managed Multi-Cloud Services involve third-party infrastructure and, by design, have certain distinct characteristics.

1. Additional Definition.

- “*Google-Managed MCS Data Processing Amendment*” means the terms at <https://cloud.google.com/terms/mcs-data-processing-terms>.

2. Multi-Cloud Data Processing Terms. The Google-Managed MCS Data Processing Amendment supplements and amends this Addendum with respect to Google-Managed Multi-Cloud Services for Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Google may not have access to Customer's VMware environment or be able to encrypt personal data in Customer's VMware environment.

NetApp Volumes (Google Cloud Platform)

1. Amendments. This Addendum is amended as follows with respect to NetApp Volumes:

- The definition of “Google's Third-Party Auditor” is replaced with the following:
 - “*Google's Third Party Auditor*” means a qualified and independent third party auditor appointed by Google or a NetApp Volumes Subprocessor, whose then-current identity Google will disclose to Customer on request.
- Section 3(a) (Data Storage, Isolation and Logging) of Appendix 2 (Security Measures) is replaced with the following:
 - (a) *Data Storage, Isolation and Logging.* Google stores data in a multi-tenant environment on servers owned by NetApp, Inc. Subject to any Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data. Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.

2. Compliance Certifications and SOC Reports. Google or its Subprocessor will obtain at least the following (or an equivalent or enhanced alternative) for NetApp Volumes:

- a. a certificate for ISO 27001 and a PCI DSS Attestation of Compliance (the “*NetApp Compliance Certifications*”); and
- b. SOC 1 and SOC 2 Reports updated annually based on an audit performed at least once every 12 months (the “*NetApp SOC Reports*”).

3. Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Addendum, Google will make any NetApp Compliance Certifications and NetApp SOC Reports available for review by Customer and, if

Customer is a processor, allow Customer to request access for the third-party controller to the NetApp SOC Reports in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

Google Workspace and Cloud Identity

1. Additional Definitions.

- “*Account*”, if not defined in the Agreement, means Customer’s Google Workspace or Cloud Identity account.
- “*Cloud Identity*” when purchased under a standalone Agreement and not as part of Google Cloud Platform or Google Workspace, means the Cloud Identity Services described at <https://cloud.google.com/terms/identity/user-features>.
- “*Customer Data*”, if not defined in the Agreement, means data submitted, stored, sent or received by or on behalf of Customer or its End Users via Google Workspace or Cloud Identity under the Account.
- “*Google Workspace*” means the Google Workspace or Google Workspace for Education services described at https://workspace.google.com/terms/user_features.html, as applicable.

2. Additional Products. If Google at its option makes Additional Products available to Customer for use with Google Workspace or Cloud Identity in accordance with applicable Additional Product Terms:

- a. Customer may enable or disable Additional Products via the Admin Console and will not need to use Additional Products in order to use Google Workspace or Cloud Identity; and
- b. if Customer opts to install any Additional Products or to use them with Google Workspace or Cloud Identity, the Additional Products may access Customer Data as required to interoperate with Google Workspace or Cloud Identity, as applicable.

For clarity, this Addendum does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products.

3. Compliance Certifications. The Compliance Certifications for Google Workspace and Cloud Identity Audited Services will also include certificates for ISO 27017 and ISO 27018.

4. Data Center Locations. The locations of Google Workspace and Cloud Identity data centers are described at <https://www.google.com/about/datacenters/locations/>.

5. Information about Subprocessors. Names, locations, and activities of Google Workspace and Cloud Identity Subprocessors are described at <https://workspace.google.com/intl/en/terms/subprocessors.html>.

6. Cloud Data Protection Team. The Data Protection Team for Google Workspace and Cloud Identity (while Administrators are signed in to their Admin Account) can be contacted at https://support.google.com/a/contact/googlecloud_dpr.

7. Additional Security Measures. For Google Workspace and Cloud Identity:

- a. Google logically separates each End User’s data from the data of other End Users; and
- b. data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared).

8. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures is available at cloud.google.com/privacy/.

9. Service Data Addendum. If Google makes an optional Service Data Addendum available for acceptance by Customer in relation to this Addendum, availability of that optional addendum will constitute a “DPA Update” if such term is defined in any Service Data Addendum previously entered into by Customer.

10. Service Specific Terms.

AppSheet (Google Workspace)

1. Amendments. This Addendum is amended as follows with respect to AppSheet:

- The paragraph titled “Server Operating Systems” in Section 1(a) of Appendix 2 (Security Measures) is replaced with the following:
 - *Server Operating Systems.* Google servers use a Linux based implementation customized for the application environment.

2. Additional Data Center Locations. Additional data center locations for AppSheet are described at <https://cloud.google.com/about/locations/>.

Looker (original)

1. Additional Definitions.

- “*Admin Console*” means any admin console applicable to each Instance.
- “*Google-Managed MCS Data Processing Amendment*” means, if applicable, the terms at <https://cloud.google.com/terms/mcs-data-processing-terms>.
- “*Google-Managed Multi-Cloud Services*” means, if applicable, specified Google services, products and features that are hosted on the infrastructure of a third party cloud provider.
- “*Looker (original)*” means an integrated platform (including cloud-based infrastructure, if applicable, and software components including any associated APIs) that enables businesses to analyze data and define business metrics across multiple data sources made available by Google to Customer under the Agreement. Looker (original) excludes Third-Party Offerings.
- “*Multi-Cloud Service Third-Party Provider*” has the meaning given in the Google-Managed MCS Data Processing Amendment.
- “*Order Form*” has the meaning given in the Agreement, unless Customer has purchased via a reseller or online marketplace or is using Looker only for trial or evaluation purposes under a trial or evaluation agreement, in which case Order Form may mean another written form (email or other electronic means permitted) as authorized by Google.

2. Amendments. This Addendum is amended as follows with respect to Looker (original):

- The definition of “Notification Email Address” is replaced with the following:
 - “Notification Email Address” means the email address(es) designated by Customer in the Order Form or via Looker (as applicable) to receive certain notifications from Google.
- The definitions of “SCCs (Controller-to-Processor)”, “SCCs (Processor-to-Controller)”, “SCCs (Processor-to-Processor)” and “SCCs

(Processor-to-Processor, Google Exporter)” in Appendix 3 (Specific Privacy Laws) are replaced with the following:

- “SCCs (*Controller-to-Processor*)” means the terms at <https://cloud.google.com/terms/looker/legal/sccs/eu-c2p>;
- “SCCs (*Processor-to-Controller*)” means the terms at <https://cloud.google.com/terms/looker/legal/sccs/eu-p2c>;
- “SCCs (*Processor-to-Processor*)” means the terms at <https://cloud.google.com/terms/looker/legal/sccs/eu-p2p>; and
- “SCCs (*Processor-to-Processor, Google Exporter*)” means the terms at <https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group>.
- The following words are added to the end of Section 10.1 (Data Storage and Processing Facilities): “or where any Multi-Cloud Service Third-Party Providers maintain facilities.”

3. Additional Customer Security Responsibilities. Customer is responsible for the security of Customer's environment, databases, and configuration for Looker (original) excluding systems managed and controlled by Google.

4. Compliance Certifications and SOC Reports. The Compliance Certifications and SOC Reports for Looker (original) Audited Services may vary according to the hosting environment in which the relevant Services are used. Google will provide details of the Compliance Certifications and SOC Reports available for specific hosting environments on request.

5. Data Center Locations. The locations of Looker (original) data centers will be described on the applicable Order Form or otherwise identified by Google.

6. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for Looker (original).

7. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures for Looker (original) is available at <https://docs.looker.com>.

8. Information about Subprocessors. Names, locations and activities of Subprocessors for Looker (original) are described at:

- a. <https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors> and
- b. <https://cloud.google.com/terms/subprocessors>.

9. Google-Managed Multi-Cloud (Looker (original))

Google-Managed Multi-Cloud Services involve third-party infrastructure and, by design, have certain distinct characteristics.

9.1 Multi-Cloud Data Processing Terms. The Google-Managed MCS Data Processing Amendment supplements and amends this Addendum with respect to Google-Managed Multi-Cloud Services for Looker (original).

10. Cloud Data Protection Team. The Data Protection Team for Looker (original) can be contacted at <https://support.google.com/cloud/contact/dpo>.

11. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

- 12. Additional Application Security Measures.** Google will implement and maintain the additional Security Measures described below for Looker (original):
- Google follows at least industry standard practices for security architecture. Proxy servers used for Google's applications help secure access to Looker by providing a single point to filter attacks through IP denylisting and connection rate limiting.
 - Customer administrators control access to applications by Google personnel to provide technical support requested by Customer or End Users.

SecOps Services

1. Additional Definitions.

- “*Account*”, if not defined in the Agreement, means Customer's SecOps Services or Google Cloud Platform account, as applicable.
- “*Customer Data*”, if not defined in the Agreement, means (i) data provided to Google by Customer or End Users through SecOps Services under the Account and data that Customer or End Users derive from that data through their use of the SecOps Services, or (ii) for Mandiant Consulting Services and Managed Services only, data provided to Google by Customer or End Users in connection with receiving SecOps Services.
- “*Customer-Engaged Provider*” means a service provider (which may include a processor or subprocessor) directly engaged by Customer under a separate agreement between Customer and such provider.
- “*SecOps Services*” means the SecOps Services described at <https://cloud.google.com/terms/secops/services>, excluding any Third-Party Offerings.
- “*Third-Party Offerings*”, if not defined in the Agreement, means (a) third-party services, software, products, and other offerings that are not incorporated into SecOps Services or Software, and (b) third-party operating systems.

2. Amendments. This Addendum is amended as follows with respect to SecOps Services:

- The definition of “Additional Security Controls” is replaced with the following:
 - “*Additional Security Controls*” means security resources, features, functionality and/or controls (if any) that Customer may use at its option and/or as it determines, including (if any) encryption, logging and monitoring, identity and access management, and security scanning.
- The definitions of “SCCs (Controller-to-Processor)”, “SCCs (Processor-to-Controller)”, “SCCs (Processor-to-Processor)” and “SCCs (Processor-to-Processor, Google Exporter)” in Appendix 3 (Specific Privacy Laws) are replaced with the following:
 - “SCCs (Controller-to-Processor)” means the terms at <https://cloud.google.com/terms/secops/sccs/eu-c2p>;
 - “SCCs (Processor-to-Controller)” means the terms at <https://cloud.google.com/terms/secops/sccs/eu-p2c>;
 - “SCCs (Processor-to-Processor)” means the terms at <https://cloud.google.com/terms/secops/sccs/eu-p2p>; and
 - “SCCs (Processor-to-Processor, Google Exporter)” means the terms at <https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter>.
- Section 6.1 (Deletion by Customer) is modified to read as follows:
 - **6.1 Deletion by Customer.** Google will enable Customer to delete Customer Data during the Term in a manner consistent with the

functionality of the Services or upon request. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, or if Customer requests deletion of any Customer Data during the Term, this use or request (as applicable) will constitute an Instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law. Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

- Section 9.1 (Access; Rectification; Restricted Processing; Portability) is modified to read as follows:
9.1 Access; Rectification; Restricted Processing; Portability. During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including as described in Section 6.1 (Deletion by Customer), and to export Customer Data upon request. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for notifying Google and Google will assist Customer in rectifying that data if required by Applicable Privacy Law.

3. Data Center Locations. The locations of SecOps Services data centers are described at <https://www.google.com/about/datacenters/locations/>.

4. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for SecOps Services.

5. Information about Subprocessors. Names, locations, and activities of Subprocessors for SecOps Services are described at <https://cloud.google.com/terms/secops/subprocessors>.

6. Cloud Data Protection Team. The Data Protection Team for SecOps Services can be contacted at <https://support.google.com/cloud/contact/dpo> (and/or via such other means as Google may provide from time to time).

7. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

8. Service Specific Terms.

Mandiant Consulting Services and Managed Services

Mandiant Consulting Services and Managed Services provide advisory and implementation services (including incident response, strategic readiness, and technical assurance to mitigate threats and reduce incident-related risks) and managed detection and response services and by design, have certain distinct characteristics.

1. Amendments. The Addendum is amended as follows solely with respect to Mandiant Consulting Services and Managed Services:

- The definition of “Data Incident” is supplemented with the following:
 - For clarity, Data Incident excludes incidents that are the subject of the Mandiant Consulting Services and/or Managed Services, as applicable.
- Section 5.2(b)(i) (Compliance with Customer’s Instructions) is replaced with the following:
 - i. Customer’s use of the Services; and
- The second sentence of Section 7.1.1 (Google’s Security Measures) is modified to read as follows:
 - The Security Measures may include (as appropriate) measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google’s systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness.
- Section 7.3.1(b) is modified to read as follows:
 - b. administering, managing access to and securing the account authentication credentials, systems, software, networks and devices that Customer uses to receive, or authorizes Google to access in order to provide, the Mandiant Consulting Services and/or Managed Services, as applicable;
- New Sections 7.3.1(d) and (e) are added as follows:
 - d. minimizing the amount of Customer Data provided by or on behalf of Customer to Google; and
 - e. to the extent Google’s access to Customer Data is within Customer’s control, revoking that access when Google has completed the Mandiant Consulting Services and/or Managed Services, as applicable.
- Appendix 2 (Security Measures) is replaced with the following:
 - Appendix 2: Additional Technical and Organizational Measures
 1. Customer-Controlled Environment. Google will only access and process Customer Data provided by or on behalf of Customer to Google via a Customer-controlled or Customer-approved account or environment.
 2. Data Access Processes and Policies – Access Policy. Google’s data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data. Google (i) only allows persons to access data they are authorized to access; and (ii) takes steps to ensure that personal data cannot be read, copied, altered or removed without authorization during processing and use. Google’s granting or modification of access rights is based on Customer’s provision to Google of end user access to its account or environment.
 3. Personnel Security. Google personnel are required to conduct themselves in a manner consistent with the company’s guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to

the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., certifications). Google's personnel will not process Customer Data without authorization.

4. Additional Security Measures. Google and Customer may agree to additional security measures in the applicable Order Form, including any attached Statement of Work, for the Mandiant Consulting Services and/or Managed Services, as applicable.

2. Customer-Engaged Provider. For clarity, and without limiting Google's obligations under Section 7 (Data Security) or 11 (Subprocessors), Appendix 2 (Security Measures) does not describe the security measures or controls implemented or provided by Customer or Customer-Engaged Providers.

Implementation Services

1. Additional Definitions.

- "*Customer Data*" means data that Customer authorizes Google Personnel to access on Customer-Managed Systems.
- "*Customer-Managed Systems*" means the following, as used by Customer to receive Implementation Services: (a) Customer-managed instances of Google Cloud Services or third-party cloud services; and (b) any hardware or software hosted or managed in Customer's on-premises environment.
- "*Google Cloud Services*" means any Services described in this Appendix 4 (Specific Products), other than Implementation Services, Mandiant Consulting Services and Mandiant Managed Services.
- "*Google Personnel*" means Google employees and contractors engaged in providing Implementation Services.
- "*Implementation Services*" means advisory, consulting and implementation services provided by Google employees and contractors in support of Google Cloud Services as described in the Agreement, including in an Order Form or a Statement of Work.

2. Amendments. This Addendum is amended as follows with respect to Implementation Services:

- The definition of "Additional Security Controls" is deleted.
- The definition of "Data Incident" is replaced with the following:
 - "*Data Incident*" means a breach of Section 7.1 (Google's Security Measures, Controls and Assistance) by Google Personnel, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
- Subject to the remainder of this section, the term "Customer Data" is replaced with "Customer Personal Data" when used (a) in Section 2 (Definitions) in the definition of "Subprocessor", and (b) in other sections of this Addendum. For clarity, other definitions in Section 2 (Definitions) remain unamended.
- Section 3 (Duration) is replaced with the following:

- **3. Duration.** Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Google no longer has access to any Customer Personal Data.
- Section 6 (Data Deletion) is replaced with the following:
 - **6. Data Deletion.** At the end of the Term, Customer will (a) determine whether to delete any Customer Personal Data, and (b) be responsible for any such deletion.
- The second sentence of Section 7.1.1 (Google's Security Measures) is replaced with the following:
 - "The Security Measures may include (as appropriate) measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness."
- Section 7.1.3 (Additional Security Controls) is deleted, together with all other references to that section.
- Section 9.1 (Access; Rectification; Restricted Processing; Portability) is replaced with the following:
 - **9.1 Access; Rectification; Restricted Processing; Portability.** Customer will be responsible for using the functionality of the Customer-Managed Systems to access, rectify and restrict processing of Customer Personal Data, including if Customer becomes aware that any Customer Personal Data is inaccurate or outdated and is required by Applicable Privacy Law to rectify or delete that data.
- Section 11.4 (Opportunity to Object to Subprocessors) is replaced with the following:
 - **11.4 Opportunity to Object to Subprocessors.** When any New Subprocessor is engaged during the Term, Google will notify Customer of the engagement of the New Subprocessor before it processes Customer Personal Data. Customer may object to the New Subprocessor by notifying Google and, if Customer does so, the parties will work in good faith to determine a mutually acceptable alternative.
- Appendix 1 (Subject Matter and Details of Data Processing) is amended as follows:
 - The "Duration of the Processing" section is replaced with the following:
 - *"Duration of the Processing.* The Term plus (if applicable) the period from the end of the Term until the expiry of Google's access to any Customer Personal Data."
 - The words "provided to Google via the Services" in the "Categories of Data" and "Data Subjects" sections are replaced with "made accessible to Google in connection with the Services".
- Appendix 2 (Security Measures) is replaced with the following:
 - **Appendix 2: Security Measures**
 - 1. Customer-Managed Systems.** Google Personnel will only access and process Customer Personal Data on Customer-Managed Systems. If those systems include Google Cloud Services, Customer's use of Google Cloud Services remains governed by the agreement applicable to those services.

2. Access Control. Google's internal data access processes and policies are designed to prevent unauthorized persons and systems from gaining access to Google Cloud Services used to process personal data. Google policies (i) only allow Google Personnel to access data they are authorized to access; and (ii) require that Google Personnel do not read, copy, alter or remove Customer Personal Data without authorization during processing, use and after recording. Customer controls the provisioning or modification of end user access rights to Customer-Managed Systems. If those systems include Google Cloud Services, details regarding workflow tools that maintain audit records of changes and system access logs are addressed in the agreement for the applicable Google Cloud Services.

3. Personnel Security. Google Personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Google Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Google Personnel are provided with security training. Google Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role (e.g., certifications).

4. Additional Security Measures. Google and Customer may agree to additional security measures in the Agreement, including in an Order Form or a Statement of Work.

5. Subprocessor Security. Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

3. Customer Security Responsibilities. In addition to its obligations under Section 7.3.1 (Customer's Security Responsibilities), Customer is responsible for the following:

- administering, managing access to, and securing Customer-Managed Systems, including minimizing Google Personnel's access to Customer Personal Data to the extent reasonably practicable and terminating that access on completion of the Implementation Services; and
- implementing any security recommendations provided in writing by Google to Customer with respect to Customer-Managed Systems.

4. Compliance Certification. Google will maintain certificates for ISO 27001, ISO 27017 and ISO 27018 covering Implementation Services provided in support of Google Cloud Platform and Google Workspace (the "*Implementation Services Compliance Certifications*"). Google may add standards at any time. Google may

replace an Implementation Services Compliance Certification with an equivalent or enhanced alternative.

5. Reviews of Compliance Certification. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the Implementation Services Compliance Certification available for review by Customer and, if Customer is a processor, allow Customer to request access for the third-party controller to the Implementation Services Compliance Certification.

6. Data Processing Locations. Customer Personal Data may be processed in any country where Google provides Implementation Services or where Customer maintains Customer-Managed Systems.

7. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for Implementation Services.

8. Information about Subprocessors. Subprocessors for Implementation Services will be identified (as subcontractors) in an applicable Order Form, Statement of Work, or other confirmation provided to Customer before commencement of the Implementation Services or will be Google Affiliates. Google will also make names, locations and activities of Subprocessors for Implementation Services available to Customer upon request.

9. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

Google Skills for Organizations

1. Additional Definitions.

- “*Account*”, if not defined in the Agreement, means Customer’s Google Skills for Organizations Customer Account.
- “*GSO*” means educational, training, and learning services and content provided through <https://skills.google> (or another website operated or controlled by Google and used for purposes of Google Skills for Organizations).
- “*TSS*” means technical support services that Google, in its discretion, may provide to Customer.

2. Amendments. This Addendum is amended as follows with respect to GSO:

- The definition of “Additional Security Controls” is replaced with the following:
 - “*Additional Security Controls*” means security resources, features, functionality and/or controls (if any) that Customer may use at its option and/or as it determines, including (if any) encryption, logging and monitoring, identity and access management, and security scanning.

- The definitions of “SCCs (Controller-to-Processor)”, “SCCs (Processor-to-Controller)”, “SCCs (Processor-to-Processor)” and “SCCs (Processor-to-Processor, Google Exporter)” in Appendix 3 (Specific Privacy Laws) are replaced with the following:
 - “SCCs (Controller-to-Processor)” means the terms at <https://cloud.google.com/terms/skills-for-organizations/sccs/eu-c2p>;
 - “SCCs (Processor-to-Controller)” means the terms at <https://cloud.google.com/terms/skills-for-organizations/sccs/eu-p2c>;
 - “SCCs (Processor-to-Processor)” means the terms at <https://cloud.google.com/terms/skills-for-organizations/sccs/eu-p2p>; and
 - “SCCs (Processor-to-Processor, Google Exporter)” means the terms at <https://cloud.google.com/terms/skills-for-organizations/sccs/eu-p2p-intra-group>.

3. Data Center Locations. The locations of GSO data centers are described at <https://cloud.google.com/about/locations/>.

4. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for GSO.

5. Information about Subprocessors. Names, locations, and activities of GSO Subprocessors are described at:

- a. <https://cloud.google.com/terms/skillsboost-organizations/subprocessors>; and
- b. <https://cloud.google.com/terms/subprocessors>.

6. Cloud Data Protection Team. The Data Protection Team for GSO can be contacted at <https://support.google.com/qwiklabs> (and/or via such other means as Google may provide from time to time).

7. Google’s Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

Previous versions of Data Processing and Security Terms:

April 9, 2024 June 30, 2022 September 24, 2021 August 19, 2020 August 10, 2020 July 17, 2020 October 11, 2019 October 1, 2019 May 25, 2018 March 13, 2018 November 9, 2017 October 11, 2017 February 7, 2017 October 6, 2016

Previous versions of Data Processing Amendment:

July 7, 2022 September 24, 2021 May 27, 2021 October 29, 2019 May 25, 2018 April 25, 2018 July 11, 2017 November 28, 2016 January 7, 2016 April 24, 2015 April 1, 2014 November 14, 2012

Previous versions of Data Processing Addendum for Looker (original) Services (Customers):

February 14, 2023 January 4, 2023 September 20, 2022 June 30, 2022 March 16, 2022 September 24, 2021 April 1, 2021 January 15, 2021 December 17, 2020 August 28, 2020 June 1, 2020 March 9, 2020

Previous versions of SecOps Services DPST (Customers):

February 6, 2023 November 28, 2022 September 27, 2021 October 1, 2020



Previous versions of Data Processing Addendum for SecOps Consulting Services and Managed Services:

October 5, 2023 September 19, 2023 June 15, 2023 February 22, 2023 February 6, 2023

Previous versions (Last modified October 23, 2025)

October 13, 2025 August 21, 2025 October 15, 2024 September 26, 2024

September 9, 2024 August 5, 2024 May 23, 2024 April 9, 2024 November 8, 2023

August 15, 2023 September 20, 2022



Google Cloud Acceptable Use Policy

For translations of this Acceptable Use Policy into other languages, please click on the appropriate link: Bahasa Indonesia (<https://services.google.com/fh/files/misc/id-cloud-acceptable-use-policy.pdf>), Deutsch (<https://services.google.com/fh/files/misc/de-cloud-acceptable-use-policy.pdf>), Español (Latinoamérica) (<https://services.google.com/fh/files/misc/es-419-cloud-acceptable-use-policy.pdf>), Français (<https://services.google.com/fh/files/misc/fr-cloud-acceptable-use-policy.pdf>), Italiano (<https://services.google.com/fh/files/misc/it-cloud-acceptable-use-policy.pdf>), Nederlands (<https://services.google.com/fh/files/misc/nl-cloud-acceptable-use-policy.pdf>), Português (<https://services.google.com/fh/files/misc/pt-br-cloud-acceptable-use-policy.pdf>), 한국어 (<https://services.google.com/fh/files/misc/ko-cloud-acceptable-use-policy.pdf>), 日本語 (<https://services.google.com/fh/files/misc/ja-cloud-acceptable-use-policy.pdf>)

Use of the Services is subject to this acceptable use policy ("AUP").

If not defined here, capitalized terms have the meaning stated in the applicable contract ("Agreement") between the customer, reseller or other authorized user ("You") and Google.

You agree not, and not to allow third parties or Your End Users, to use the Services:

- to violate, or encourage the violation of, the legal rights of others;
- to engage in, promote, or encourage illegal activity, including child sexual exploitation, child abuse, or terrorism or violence that can cause death, serious harm, or injury to individuals or groups of individuals;
- for any unlawful, invasive, infringing, defamatory, or fraudulent purpose including Non-consensual Explicit Imagery (NCEI), violating intellectual property rights of others, phishing, or creating a pyramid scheme;
- to distribute viruses, worms, Trojan horses, corrupted files, hoaxes or other items of a destructive or deceptive nature;
- to gain unauthorized access to, disrupt, or impair the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
- to alter, disable, interfere with or circumvent any aspect of the Services, Software, or the equipment used to provide the Services;
- to generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisements, or other solicitations ("spam");
- to test or reverse-engineer the Services in order to find limitations or vulnerabilities, or to evade filtering capabilities, except as expressly permitted in the Agreement; or
- to use the Services, or any interfaces provided with the Services, to access any other Google product or service in a manner that violates the terms of service of such other Google product or service.

In addition, if you are using Google Workspace or Google Workspace for Education, you agree not, and not to allow third parties or Your End Users, to use the Services:

- to grant multiple individuals access to an individual End User Account other than via the delegation features provided within the Services;
- to create End User Accounts assigned to business functions rather than to human beings for the purpose of sharing files within or outside of the domain;
- to resell End User Accounts, or parts thereof, as added into a commercial product offered to third parties; or
- to record audio or video communications without consent if such consent is required by applicable laws and regulations (you are solely responsible for ensuring compliance with all applicable laws and regulations in the relevant jurisdiction(s)).

If You use Google Workspace for Education, You agree to use all Services, Additional Products, and Third-Party Offerings that are accessible with Your Account only (a) for educational purposes, and (b) if You are an End User, as authorized by Your school.

You will not, and will not allow End Users to, (a) copy, modify, or create a derivative work of the Services; (b) reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any or all of the source code of, the Services (except to the extent such restriction is expressly prohibited by applicable law); (c) sell, resell, sublicense, transfer, or distribute any or all of the Services; or (d) access or use the Services (i) for High Risk Activities; (ii) in violation of the AUP; (iii) in a manner intended to avoid incurring Fees (including creating multiple Customer Applications, Accounts, or Projects to simulate or act as a single Customer Application, Account, or Project (respectively)) or to circumvent Service-specific usage limits or quotas; (iv) to engage in cryptocurrency mining without Google's prior written approval; (v) to operate or enable any telecommunications service or in connection with any Customer Application that allows End Users to place calls or to receive calls from any public switched telephone network, unless otherwise described in the Service Specific Terms; (vi) to place or receive emergency service calls via the GWS Services, unless stated otherwise in the Service Specific Terms; (vii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (viii) in a manner that breaches, or causes the breach of, Export Control Laws; or (ix) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA.

We also expect you to comply with the Generative AI Prohibited Use Policy (<https://policies.google.com/terms/generative-ai/use-policy>).

Your failure to comply with the AUP may result in suspension or termination, or both, of the applicable Services pursuant to the Agreement.

Previous versions (*Last modified October 13, 2025*)



July 1 2025, February 6 2023, December 16 2015, September 18 2012



Generative AI Prohibited Use Policy

Last Modified: December 17, 2024

Generative AI models can help you explore, learn, and create. We expect you to engage with them in a responsible, legal, and safe manner. The following restrictions apply to your interactions with generative AI in the Google products and services that refer to this policy.

1. Do not engage in dangerous or illegal activities, or otherwise violate applicable law or regulations. This includes generating or distributing content that:
 - a. Relates to child sexual abuse or exploitation.
 - b. Facilitates violent extremism or terrorism.
 - c. Facilitates non-consensual intimate imagery.
 - d. Facilitates self-harm.
 - e. Facilitates illegal activities or violations of law -- for example, providing instructions for synthesizing or accessing illegal or regulated substances, goods, or services.
 - f. Violates the rights of others, including privacy and intellectual property rights -- for example, using personal data or biometrics without legally-required consent.
 - g. Tracks or monitors people without their consent.
 - h. Makes automated decisions that have a material detrimental impact on individual rights without human supervision in high-risk domains -- for example, in employment, healthcare, finance, legal, housing, insurance, or social welfare.
2. Do not compromise the security of others' or Google's services. This includes generating or distributing content that facilitates:
 - a. Spam, phishing, or malware.
 - b. Abuse of, harm to, interference with, or disruption to Google's or others' infrastructure or services.
 - c. Circumvention of abuse protections or safety filters -- for example, manipulating the model to contravene our policies.
3. Do not engage in sexually explicit, violent, hateful, or harmful activities. This includes generating or distributing content that facilitates:
 - a. Hatred or hate speech.
 - b. Harassment, bullying, intimidation, abuse, or the insulting of others.
 - c. Violence or the incitement of violence.

- d. Sexually explicit content -- for example, content created for the purpose of pornography or sexual gratification.
4. Do not engage in misinformation, misrepresentation, or misleading activities. This includes:
- a. Frauds, scams, or other deceptive actions.
 - b. Impersonating an individual (living or dead) without explicit disclosure, in order to deceive.
 - c. Facilitating misleading claims of expertise or capability in sensitive areas -- for example in health, finance, government services, or the law, in order to deceive.
 - d. Facilitating misleading claims related to governmental or democratic processes or harmful health practices, in order to deceive.
 - e. Misrepresenting the provenance of generated content by claiming it was created solely by a human, in order to deceive.

We may make exceptions to these policies based on educational, documentary, scientific, or artistic considerations, or where harms are outweighed by substantial benefits to the public.

Abuse monitoring

As outlined in Section 4.3 "Generative AI Safety and Abuse" of Google Cloud Platform Terms of Service (<https://cloud.google.com/terms/>), Google uses the following process to detect potential abuse and violations of its Acceptable Use Policy (<https://cloud.google.com/terms/aup?hl=en>) and Prohibited Use Policy (<https://policies.google.com/terms/generative-ai/use-policy>) as part of providing Generative AI Services to customers.

- **Automated detection:** Google uses automated safety classifiers to detect potential abuse and violations. For technical details on how safety classifiers work, see Configure safety filters (<https://docs.cloud.google.com/vertex-ai/generative-ai/docs/multimodal/configure-safety-filters>).
- **Prompt logging:** If automated safety classifiers detect suspicious activity that requires further investigation into whether a customer has violated our policies, then Google may log customer prompts solely for the purpose of examining whether a violation of the AUP or Prohibited Use Policy has occurred. This data won't be used to train or fine-tune any AI/ML models. This data is stored securely for up to 30 days in the same region or multi-region selected by the customer for their project and adheres to Google Cloud assurances, such as Data Residency, Access Transparency and VPC Service Controls. Customers also have the option to request an opt-out from abuse logging (see below).
- **Action:** Authorized Google employees may assess the flagged prompts and may reach out to the customer for clarification. Failure to address the behavior—or recurring or severe abuse—may result in suspension or termination of the customer's access to Vertex AI or Google Cloud services.
- **Services in scope:** Vertex AI API, when used with Google's generative AI models.
- **Customers in scope:** Only customers whose use of Google Cloud is governed by the Google Cloud Platform Terms of Service (<https://cloud.google.com/terms/>).
- **Customer opt-out:** Customers may request for an exception by filling out this form (https://docs.google.com/forms/d/e/1FAIpQLSdpXIYgrSfTw_U0E_z3-RLap4YPNVw24vv2rpD0-dwTKkL0-A/viewform). If approved, Google won't store any prompts associated with the approved Google Cloud account.

What's next



- Learn about Responsible AI
(<https://docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/responsible-ai>).



SecOps Services Summary

The complete list of services that form SecOps Services is shown below. While Google offers many other services and APIs, only the services below are covered under the agreement pursuant to which Google has agreed to provide SecOps Services (the “Agreement”), service level agreements (if applicable), and support offerings. Information about SecOps packages, including the Services and functionality included in each package, is available at <https://cloud.google.com/security/products/security-operations?hl=en#pricing> or a successor URL.

Google Security Operations: Google Security Operations includes the following two Services:

Google SecOps - SIEM, a cloud native security information and event management (SIEM) solution, enables customers to collect and analyze security telemetry from across their enterprise to power detection, investigation, and remediation of threats. As part of the service, Google SecOps - SIEM normalizes, correlates, and enriches security data to provide analysis and context on suspicious activity.

Google SecOps - SOAR, a cloud native security, orchestration, automation and response (SOAR) solution, empowers security teams to respond to cyber threats in minutes. Google SecOps - SOAR fuses a unique threat-centric approach, powerful yet simple playbook automation, and context-rich investigation to free up valuable time and enable security team members to be informed, productive and effective.

Google Threat Intelligence: Google Threat Intelligence is a rich and actionable threat intelligence suite combining insights across Mandiant, VirusTotal and other Google properties. It equips security teams with comprehensive context and a cutting edge investigative workbench to proactively protect their networks from cybersecurity threats and understand the evolving threat landscape.

Mandiant Solutions: Mandiant software and cloud solutions help security teams evaluate the effectiveness of their security tools and stay ahead of sophisticated threat actors. Mandiant Solutions are in part made available through the Mandiant Advantage Platform, a multi-vendor XDR platform that delivers transformative expertise and frontline intelligence to security teams.

Mandiant Solutions include:

Mandiant Security Validation enables an organization’s security team to build a continuous and automated validation program that tests the security effectiveness of network, endpoint, email and cloud controls, teams and processes.

Mandiant Attack Surface Management helps organizations discover and analyze their internet assets across today’s dynamic, distributed, and shared environments. This service generates comprehensive visibility of the extended enterprise through continuous discovery that illuminates assets, alerts on risk and enables cyber security teams to inventory their assets and investigate any discovered exposures.



Mandiant Advantage Threat Intelligence gives security professionals critical insights into the latest relevant threats so that they can be better prepared to guard against sophisticated attacks.

Mandiant Digital Threat Monitoring gives security professionals visibility into external threats to their organization on the open, deep and dark web.

Mandiant Managed Services: Mandiant managed services act as a seamless extension of customers' security teams, delivering continuous monitoring, event triage, investigations, threat hunting, and remediation recommendations that are agnostic to customers' endpoint and network tooling. Mandiant Managed Services includes, for example, Mandiant Threat Defense.

Mandiant Consulting Services: Mandiant Consulting offers proven global expertise in providing comprehensive incident response, strategic readiness and offensive security to help customers mitigate threats and reduce business risk before, during and after an incident.

Expertise On Demand: Expertise on Demand extends security operations capabilities and capacity by providing customers with access to security resources, threat intelligence and training led by security practitioners to help accelerate response without burning out existing staff.

Training Services: Through incident response and threat intelligence teachings, and a proctor-based certifications program, Training Services, also known as Mandiant Academy, help to advance customer operational skillsets and problem-solving competencies for increased security maturity.

Security Customer Success Services: Security Customer Success Services help to enable Google Cloud Security customers to achieve desired business outcomes using their acquired subscriptions through the provision of onboarding, training, and enablement resources.

Previous versions (*Last modified April 10, 2025*)

October 30 2024, August 28 2024, July 15 2024, May 23 2024, April 4 2024, February 14 2024, February 22 2023, February 6 2023



SecOps Service Specific Terms

For translations of these SecOps Service Specific Terms into other languages, please click on the appropriate link: Bahasa Indonesia (<https://services.google.com/fh/files/misc/id-secops-service-specific-terms.pdf>), Deutsch (<https://services.google.com/fh/files/misc/de-secops-service-specific-terms.pdf>), Español (Latinoamérica) (<https://services.google.com/fh/files/misc/es-419-secops-service-specific-terms.pdf>), Français (<https://services.google.com/fh/files/misc/fr-secops-service-specific-terms.pdf>), Italiano (<https://services.google.com/fh/files/misc/it-secops-service-specific-terms.pdf>), Nederlands (<https://services.google.com/fh/files/misc/nl-secops-service-specific-terms.pdf>), Português (<https://services.google.com/fh/files/misc/pt-br-secops-service-specific-terms.pdf>), 한국어 (<https://services.google.com/fh/files/misc/ko-secops-service-specific-terms.pdf>), 日本語 (<https://services.google.com/fh/files/misc/ja-secops-service-specific-terms.pdf>).

These SecOps Service Specific Terms are incorporated into the agreement under which Google has agreed to provide SecOps Services (as described at <https://cloud.google.com/terms/secops/services>) to Customer (the “Agreement”). If the Agreement authorizes you to resell or supply SecOps Services under a Google Cloud partner or reseller program, then except for in the section entitled “Partner-Specific Terms”, all references to Customer in these SecOps Service Specific Terms refer to you (“Partner” or “Reseller”, as used in the Agreement), and all references to Customer Data in the SecOps Service Specific Terms mean Partner Data. If you are accessing the Services as a customer of an unaffiliated Google Cloud reseller, then Section 9 (Resold Customers) of the General Service Terms will apply. Capitalized terms used but not defined in the SecOps Service Specific Terms have the meaning given to them in the Agreement.

General Service Terms

1. Data

- a. *Improvements.* To respond to the evolving threat landscape and provide current and state-of-the-art cybersecurity, as part of providing the Services we process Customer Data to improve the security, threat detection, prevention, and response capabilities of such Services.
- b. *Location.* In the Order Form or by other means if made available by Google, Customer may select to store Customer Data in a specific Region or Multi-Region as detailed in the SecOps Services Locations Page (“Data Location Selection”), and Google will store that Customer Data at rest only in the selected Region/Multi-Region. Google may replicate that Customer Data within any other Region located within the country of the selected Region or within the country or countries of the selected Multi-Region (as applicable) for backup, reliability, debugging, support, maintenance, or security purposes. The Services do not limit the locations from which Customer or Customer End Users may access Customer Data or to which they may move Customer Data. For clarity, Customer Data does not include resource identifiers, attributes, or other data labels.

2. General Software Terms. The following terms apply to all Software:

- a. *License.* Google grants Customer a royalty-free (unless otherwise stated by Google), non-exclusive, non-sublicensable, non-transferable license during the Term to reproduce and use the Software ordered by Customer on systems owned, operated, or managed by or on behalf of Customer in accordance with (i) the Agreement, and (ii) if applicable, the Scope of Use. Customer may authorize its and its Affiliates' employees, agents, and subcontractors (collectively, “Software Users”) to use the Software in accordance with this section (License), so long as Customer remains responsible. Customer may make a reasonable number of copies of the Software for back-up and archival purposes. For clarity, Software does not constitute Services.
- b. *Documentation.* Google may provide Documentation describing the appropriate operation of the Software, including usage guidelines, and whether and how the Software collects and processes data. Customer will comply with any restrictions in the Documentation regarding Software use.
- c. *Compliance With Scope of Use.* Within 30 days of Google’s reasonable written request, Customer will provide a detailed written report describing its usage in accordance with the applicable Scope of Use of each Software product used by Customer and its Software Users during the requested period. If requested, Customer will provide reasonable assistance and access to information to verify the accuracy of Customer’s Software usage report(s).
- d. *Other Warranties and Compliance.* Each party represents and warrants that it will comply with all laws and regulations applicable to its provision or use of the Software, as applicable. Customer will: (i) ensure that Customer and its Software Users' use of the Software complies with the Agreement and the restrictions in the Agreement applying to Customer's use of the Services; (ii) use commercially reasonable efforts to prevent and terminate any unauthorized access to or use of the Software; and (iii) promptly notify Google of any

unauthorized access to or use of the Software of which Customer becomes aware. If the Software contains open source or third-party components, those components may be subject to separate license agreements, which Google will make available to Customer. Customer is solely responsible for complying with the terms of any third-party sources from which Customer elects to migrate its workloads onto the Services, and represents and warrants that such third-party sources permit the use of Software to migrate applications away from such sources. If the Agreement terminates or expires, then Customer will stop using all Software and delete it from Customer's systems.

3. Premium Software Terms. The following terms apply only to Premium Software:

a. *Introduction.* Google makes certain Software available under the Agreement described as “Premium Software” in an Order Form or otherwise identified as Premium Software by Google (“Premium Software”). Customer will pay applicable Fees for any Premium Software it obtains as described in the applicable Order Form. Premium Software is Google’s Confidential Information.

b. *Software Warranty.* Google warrants to Customer that for one year from its delivery, Premium Software will perform in material conformance with the applicable Documentation. This warranty will not apply if (i) Customer does not notify Google of the non-conformity within 30 days after Customer first discovers it, (ii) Customer modifies Premium Software or uses it in violation of the Agreement, or (iii) the non-conformity is caused by any third-party hardware, software, services, or other offerings or materials, in each case not provided by Google.

If Google breaches this warranty, then Google will, in its discretion, repair or replace the impacted Premium Software at no additional charge. If Google does not believe that repairing or replacing would be commercially reasonable, then Google will notify Customer and (A) Customer will immediately cease use of the impacted Premium Software and (B) Google will refund or credit any prepaid amounts for the impacted Premium Software and Customer will be relieved of any then-current commitment to pay for future use of the impacted Premium Software. Without limiting the parties’ termination rights, this section (Software Warranty) states Customer’s sole remedy for Google’s breach of the warranty in this section (Software Warranty).

c. *Software Indemnification.* Google’s indemnity obligations under the Agreement with respect to allegations of infringement of third-party Intellectual Property Rights apply to Premium Software, and Customer’s indemnity obligations under the Agreement with respect to Customer’s use of the Services apply to Customer’s use of Premium Software. In addition to any other indemnity exclusions in the Agreement, Google’s indemnity obligations will not apply to the extent the underlying allegation arises from modifications to Premium Software not made by Google or use of versions of Premium Software that are no longer supported by Google.

d. *Technical Support.* Unless otherwise specified by Google, Google will make TSS available for Premium Software for an additional charge, in accordance with the TSS Guidelines.

e. *Compliance.* Premium Software may transmit to Google metering information reasonably necessary to verify that use of the Premium Software complies with the Scope of Use, as described in the applicable Documentation.

Customer will not disable or interfere with the transmission of such metering information.

f. *Updates and Maintenance.* During the Term, Google will make available to Customer copies of all current versions, updates, and upgrades of Premium Software, promptly upon general availability, as described in the Documentation. Unless otherwise stated in the Documentation for the applicable component of Premium Software, Google will maintain the current release of Premium Software and the two versions immediately preceding the current release, including by providing reasonable bug fixes and security patches. Maintenance for any Premium Software may be discontinued with one year's notice from Google, except Google may eliminate maintenance for a version and require upgrading to a maintained version to address a material security risk or when reasonably necessary to avoid an infringement claim or comply with applicable law.

4. Pre-GA Offerings Terms. Google may make available to Customer pre-general availability features, services or software that are either not yet listed at <https://cloud.google.com/terms/secops/services> or identified as “Early Access,” “Alpha,” “Beta,” “Preview,” “Experimental,” or a similar designation in related documentation or materials (collectively, “Pre-GA Offerings”). While Pre-GA Offerings are not Services or Software, Customer's use of Pre-GA Offerings is subject to the terms of the Agreement applicable to Services (or Software, if applicable), as amended by this Section 4.

Customer may provide feedback and suggestions about the Pre-GA Offerings to Google, and Google and its Affiliates may use any feedback or suggestions provided without restriction and without obligation to Customer.

PRE-GA OFFERINGS ARE PROVIDED “AS IS” WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS OF ANY KIND. Pre-GA Offerings (a) may be changed, suspended or discontinued at any time without prior notice to Customer and (b) are not covered by any SLA or Google indemnity. Except as otherwise expressly indicated in a written notice or the documentation for a given Pre-GA Offering, (i) Pre-GA Offerings may not be covered by TSS, (ii) the Cloud Data Processing Addendum does not apply to Pre-GA Offerings and Customer should not use Pre-GA Offerings to process personal data or other data subject to legal or regulatory compliance requirements, and (iii) Google's data location commitments set out in these Service Specific Terms will not apply to Pre-GA Offerings. With respect to Pre-GA Offerings, to the maximum extent permitted by applicable law, neither Google nor its suppliers will be liable for any amounts in excess of the lesser of (A) the limitation on the amount of liability stated in the Agreement or (B) \$25,000. Nothing in the preceding sentence will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability). Customer's access to and use of any Pre-GA Offering is subject to any applicable Scope of Use. Either party may terminate Customer's use of a Pre-GA Offering at any time with written notice to the other party. Certain Pre-GA Offerings may be subject to additional terms stated below.

5. Benchmarking. Customer may conduct benchmark tests of the Services (each a “Test”). Customer may only publicly disclose the results of such Tests if it (a) obtains

Google's prior written consent, (b) provides Google all necessary information to replicate the Tests, and (c) allows Google to conduct benchmark tests of Customer's publicly available products or services and publicly disclose the results of such tests. Notwithstanding the foregoing, Customer may not do either of the following on behalf of a hyperscale public cloud provider without Google's prior written consent: (i) conduct (directly or through a third party) any Test of the Services or (ii) disclose the results of any such Test.

6. Trials. Certain Services may be made available to Customer on a trial basis under a trial account ("Trial Account"). The parameters of each trial, including any Scope of Use, may be presented to Customer through the Order Form, Documentation, email, or as otherwise communicated by Google. Use of a trial indicates Customer's acceptance of any such parameters. When the trial ends or terminates, Customer will no longer have access to the Services under the Trial Account and any Customer Data in the Services will be deleted unless Customer orders the Services before the end of the trial period.

7. Generative AI Features.

a. *Disclaimer.* Generative AI Features use emerging technology, may provide inaccurate or offensive output, and are not designed for or intended to meet Customer's regulatory, legal, or other obligations. Customer acknowledges that a Generative AI Feature may, in some scenarios, produce the same or similar output for multiple customers.

b. *Training Restriction.* Google will not use Customer Data to train or fine-tune any Generative AI/ML models without Customer's prior permission or instruction.

c. *Prohibited Use Policy.* For the purposes of Generative AI Features, the Prohibited Use Policy located at <https://policies.google.com/terms/generative-ai/use-policy>, as may be updated from time to time, is incorporated into the AUP.

d. *Competitive Use.* Customer will not, and will not allow End Users to, use the Generative AI Features or output to develop a similar or competing product or service. Google may immediately suspend or terminate Customer's use of any Generative AI Feature based on any suspected violation of the preceding sentence.

e. *Model Restrictions.* Customer will not, and will not allow End Users to, use output from Generative AI Features to: (i) substitute, replace, or circumvent the use of a Google Model, directly or indirectly, or (ii) create or improve models similar to a Google Model.

f. *No Reverse Engineering.* Customer will not, and will not allow End Users to, reverse engineer or extract any components of Generative AI Features, Software, or its models (such as using prompts to discover training data). Google may immediately suspend or terminate Customer's use of any Generative AI Features based on any suspected violation of the preceding sentence.

g. *Age Restrictions.* Customer will not, and will not allow End Users to, use a Generative AI Feature as part of a website or other online service that is directed towards or is likely to be accessed by individuals under the age of 18.

- h. *Healthcare Restrictions.* Customer will not, and will not allow End Users to, use the Generative AI Features for clinical purposes (for clarity, non-clinical research, scheduling, or other administrative tasks is not restricted), as a substitute for professional medical advice, or in any manner that is overseen by or requires clearance or approval from any applicable regulatory authority.
- i. *Suspected Violations.* Google may immediately suspend or terminate Customer's use of a Generative AI Feature based on any suspected violation of subsections (c) or (d) above.
- j. *Restrictions.* The restrictions contained in subsections (g) and (h) above are deemed to be "Restrictions" or "Use Restrictions" under the applicable Agreement.

8. Support. If Customer is not an existing Google Cloud Platform customer, then the following terms apply: To access the Technical Support Services, Customer must login to the Google Cloud Platform admin console ("GCP Admin Console") and accept the Google Cloud Platform Terms of Service at <https://cloud.google.com/terms> ("GCP Service Terms"). Access to the GCP Admin Console provides Customer's administrator with the option (and no obligation) to use certain Google Cloud Platform Services (described at <https://cloud.google.com/terms/services> (the "GCP Services")). For clarity, Customer has no obligation to purchase or use GCP Services to access or use the Technical Support Services via the GCP Admin Console, and Customer is not bound by the GCP Service Terms provided that Customer accesses the GCP Admin Console only to obtain Technical Support Services.

9. Resold Customers. This Section 9 (Resold Customers) applies only if (i) Customer orders SecOps Services from a Reseller under a Reseller Agreement (such Services, "Resold Services") and (ii) Customer has a direct agreement with Google to provision those Resold Services.

- a. *Applicable Terms.* For the purposes of Resold Services:
 - i. Any section of the Agreement titled "Payment Terms" will not apply, nor will any provisions elsewhere in the Agreement (including in these SecOps Service Specific Terms) relating to billing, invoicing, or payment;
 - ii. Reseller Fees will apply and be payable directly to Reseller, and all prices for Resold Services will be solely determined between Reseller and Customer;
 - iii. Google will provide to Customer the Resold Services described in the Reseller Order to the extent that there is a valid and binding order for such Services between Google and Reseller. Notwithstanding the foregoing, for Mandiant Consulting Resold Services, Customer may be required to enter into an Order Form directly with Google;
 - iv. Customer will receive any applicable SLA credits or monetary refunds described in the Agreement from Reseller only (and Customer must notify Reseller if Google fails to meet any SLA);
 - v. Notwithstanding Google's support obligations in the TSS Guidelines, Google will not provide any support to Customer unless (i) Customer orders TSS from Google directly or (ii) Reseller orders TSS from Google on behalf of Customer, and such TSS entitlement requires Google to provide TSS directly to Customer. All other support (if any) will be provided to Customer

- by Reseller in accordance with the Reseller Agreement, subject to Section 9(e) (Reseller Technical Support);
- vi. Customer acknowledges that access to the Services may be Suspended if at any time Reseller or Customer fails to maintain a billing account linked to Customer's Account;
- vii. In the event of termination of the Agreement, Google will send Reseller (and not Customer) the final invoice (if applicable) for payment obligations related to Resold Services. Customer will notify (i) Reseller of any termination of the Agreement and (ii) Google of any termination of the Reseller Agreement;
- viii. Any renewal(s) of the Resold Services and/or any Reseller Order will be as agreed between Customer and Reseller;
- ix. If Reseller fails to pay an undisputed invoice for Resold Services to Google due to Customer's failure to pay Reseller, Google may Suspend Customer's access to the Services;
- x. To the extent that any Customer Data is under Reseller's organizational resource, then notwithstanding anything to the contrary in this Agreement (including the Cloud Data Processing Addendum):
- (A) the Cloud Data Processing Addendum will not apply with respect to the processing and security of such Customer Data;
 - (B) Google will only access, use, and otherwise process such Customer Data in accordance with the separate agreement between Google and Reseller (including its then-current terms describing data processing and security of "Partner Data" as defined by that agreement) and will not access, use, or process such Customer Data for any other purpose; and
 - (C) the consents and notices for which Customer is responsible under the section of this Agreement titled "Privacy" or "Consents" must also permit accessing, storing, and processing of Customer Data as described in subsection (B) above.
- xi. Certain SecOps Services require linking to the Reseller's billing account in order to be billed by the Reseller. Customer acknowledges and agrees that, (A) if Google's agreement with the Reseller or Customer's Reseller Agreement is terminated or expires, then the Services will no longer be linked to the Reseller's billing account, and (B) unless any such Services used by Customer are linked to the Reseller's billing account, such Services will (x) not constitute Resold Services (and therefore not be subject to this Section 9 (Resold Customers)), and (y) be regarded as Services ordered directly from Google and accordingly, despite the terms of the Reseller Agreement (including the fees agreed between Customer and Reseller), Customer will be required to pay Fees to Google for such Services, in accordance with the terms of this Agreement. For inquiries about which SecOps Services must be linked, Customer should contact Reseller.
- xii. "Cloud Data Processing Addendum," as it is used in this Agreement, means the then-current terms describing data processing and security obligations with respect to Customer Data that is (i) under Customer's (and not Reseller's) organizational resource or (ii) related to Mandiant Consulting Resold Services or Mandiant Managed Resold Services, as described at <https://cloud.google.com/terms/data-processing-addendum/>.

- xiii. “Order Term,” as it is used in this Agreement, means the period of time starting on the Services Start Date or the renewal date (as applicable) for the Resold Services and continuing until the expiration or termination of the applicable Reseller Order;
- xiv. “Services Start Date,” as it is used in this Agreement, means either the start date described in the Reseller Order or, if none is specified in the Reseller Order, the date Google makes the Resold Services available to Customer; and
- b. *Liability Cap.* For the purposes of the section of the Agreement titled “Limitation on Amount of Liability”, where the event giving rise to Liability is a breach of this Agreement or otherwise arises in connection with the Resold Services, “Fees” as it is used in that Section means “Reseller Fees”. If Customer or Google brings a claim under the Agreement, then for the purposes of establishing the Liability cap under the section of the Agreement titled “Limitation on Amount of Liability”, upon Google's request, Customer will (i) promptly disclose to Google the amount of any Reseller Fees paid or payable under the Reseller Agreement; (ii) consent to Reseller disclosing such amount to Google, notwithstanding Reseller's confidentiality obligations under the Reseller Agreement; and (iii) procure any consents necessary to enable Customer's or Reseller's disclosure under this Section 9(b) (Liability Cap). Subject to the section of the Agreement titled “Unlimited Liabilities”, Google will not be liable for damages under this Agreement to the extent Customer has claimed damages from Reseller in respect of the same event or series of events.
- c. *Sharing Confidential Information.* Google may share Customer Confidential Information with Reseller as a Delegate subject to the section of the Agreement titled “Confidentiality” or “Confidential Information”.
- d. *Reseller-Customer Relationship.* At Customer's discretion, Reseller may access Customer's Account. As between Google and Customer, Customer is solely responsible for (i) any access by Reseller to Customer's Account; (ii) defining in the Reseller Agreement any rights or obligations as between Reseller and Customer with respect to the Resold Services; and (iii) verifying whether data provided to Google by Customer or End Users through the Resold Services (other than Mandiant Consulting Resold Services or Mandiant Managed Resold Services) under the Account or derived by Customer or End Users from that data through their use of such Resold Services will be under Customer's or Reseller's organizational resource. Google will not have any Liability arising out of a Reseller's (x) suspension or termination of Customer's access to the Services; (y) access to and visibility of Customer's Account and Customer's Account's billing-related metadata; or (z) offering or provisioning of Reseller or third party products or services.
- e. *Reseller Technical Support.* Customer acknowledges and agrees that Reseller may disclose Customer and End User personal data to Google as reasonably required for Reseller to handle any support issues that Customer escalates to or via Reseller.
- f. *Survival.* The following subsections of this Section 9 (Resold Customers) will survive expiration or termination of the Agreement: Section 9(a)(vii) (termination of Reseller Agreement), Section 9(b) (Liability Cap), Section 9(c)

(Sharing Confidential Information), and Section 9(d) (Reseller-Customer Relationship).

10. Currency Conversion. When charging in non-USD currency, Google will convert USD-denominated prices into applicable currency according to market conversion rates published by leading financial institutions from time to time.

11. Additional Definitions.

“Documentation” means the Google documentation (as may be updated from time to time) in the form generally made available by Google to Customer for use with the applicable Services, as defined for each SecOps Service in the applicable Service Terms below.

“Generative AI Feature(s)” means any generative AI feature of a Service.

“Google Models” means a model trained by Google and not released as an open model under an open source or other license.

“Multi-Region” means a defined set of Regions.

“Reseller” means, if applicable, the authorized unaffiliated third-party reseller that sells the Services to Customer.

“Reseller Agreement” means, if applicable, the separate agreement between Customer and Reseller regarding the Services. The Reseller Agreement is independent of and outside the scope of this Agreement.

“Reseller Fees” means the fees (if any) for Services used or ordered by Customer as agreed in a Reseller Agreement, plus any applicable Taxes.

“Reseller Order” means, if applicable, an order form issued by a Reseller and executed by Customer and the Reseller specifying the Services Customer is ordering from the Reseller.

“Region” means a region from which a particular Service is offered, as identified at the SecOps Services Locations Page.

“Scope of Use” means any limits on installation or usage of Services or Software presented by Google.

“SecOps Services Locations Page” means

<https://cloud.google.com/terms/secops/data-residency>.

As used throughout these Service Specific Terms, “Cloud Data Processing Addendum” (formerly referred to as the Data Processing and Security Terms) has the meaning given in the Agreement or, if no such meaning is given, means the then-current terms describing data processing and security obligations with respect to Customer Data, at <https://cloud.google.com/terms/data-processing-addendum>.

If Customer is ordering SecOps Services from a Reseller under a Reseller Agreement, then all references to “Order Form” in these SecOps Service Specific Terms means an order form, statement of work, or other ordering document issued by Google and executed by Reseller and Google in relation to Resold Services.

Service Terms

The following terms apply only to the Service(s) indicated in the section title.

1. Google Security Operations (Google SecOps - SIEM / Google SecOps - SOAR)

a. **Service Models.** Google Security Operations is available in the following service models, as specified in an Order Form:

i. *Data Ingestion (Log Ingest).* Customers are charged a flat rate based on data ingestion up to the Data Cap. The following terms apply to this service model:

A. *Overages.* The applicable Order Form will identify Customer's Data Cap as the number of Units purchased. In the event Customer consumed in excess of the Units purchased (as determined in Google's sole discretion), Google will invoice Customer in arrears at the end of each month for any Units that Customer consumes in excess of the Units purchased, which will be charged at the monthly-prorated List Price less the applicable Discount as set forth in the applicable Order Form, unless otherwise agreed by the parties in writing. Customer will pay such invoice by the Payment Due Date. If Customer does not pay such invoice within thirty (30) days of the Payment Due Date, then Google may terminate the applicable Order Form upon written notice to Customer.

ii. *Covered Personnel.* Customers are charged a flat rate per each Covered Personnel. The following terms apply to this service model:

A. *Data Limitations.* Google Security Operations is only to be used for Network Telemetry and Third Party Telemetry. Customer agrees that it will not provide any data to Google Security Operations that is not Network Telemetry or Third Party Telemetry. Customer further agrees to work with Google to filter Customer Data that does not constitute Network Telemetry or Third Party Telemetry.

B. *Overages.* The applicable Order Form will identify the number of Covered Personnel as the number of Units purchased. Overages in the number of Covered Personnel are subject to proportional increases in Customer's Fees during an Order Term based on any ten percent (10%) or more increase in Covered Personnel from the number reported in an Order Form.

C. *Compliance.* Within 30 days of Google's reasonable written request, Customer will provide documentation establishing that the number of Covered Personnel providing Customer Data to Google Security Operations does not exceed the number of Units reported in an Order Form plus ten percent (10%).

b. **Service Suspension.** Google may Suspend Customer's access to Google Security Operations if Customer does not comply with the data limitations provision in Section 1(a)(ii)(A) of these Google Security Operations Service Terms, and Customer's non-compliance is not cured following notice from Google within the Data Limitation Notice Period. If Google Suspends Customer's access to Google Security Operations under this Section, then (i) Google will provide Customer notice of Suspension without undue delay, to the

extent legally permitted, and (ii) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

c. **Data Period.** Subject to and in accordance with the Cloud Data Processing Addendum, (i) Google will maintain Customer Data in Google Security Operations for the Data Period so long as Customer has an active subscription, and (ii) Customer instructs Google that it may delete Customer Data (A) upon termination or expiration of Customer's subscription (even if the Data Period extends beyond such term); and (b) that is outside the Data Period.

d. **Third-Party and Supplemental Terms.**

i. **Third-Party Offerings.** Customer must obtain access to any Third-Party Offerings from the respective provider (a "Third-Party Provider"). To the extent Customer provides access to the Customer's Account to a Third-Party Offering or Third-Party Provider, Customer explicitly consents and instructs Google to allow the Third-Party Provider of any such Third-Party Offerings to access Customer Data as may be required to interact with Google Security Operations, including to copy Customer Data into or out of Google Security Operations. For clarity, Third-Party Providers are not Subprocessors (as defined in the Cloud Data Processing Addendum).

A. **Disclaimers.** The manner in which Third-Party Offerings and Third-Party Providers transmit, use, store, and disclose Customer Data is governed solely by the policies of such Third-Party Offering and Third-Party Provider. To the extent permitted under applicable law, Google will have no liability or responsibility for:

1. Customer's use of a Third-Party Offering, including any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such Third-Party Offering, any non-Google integrations of the Services with Third-Party Offerings, actions or the effect of actions that Customer authorizes Google to take with respect to Third-Party Offerings and a Third-Party Provider's access to and use of Customer Data;
2. the privacy practices or other actions of any Third-Party Offering or Third-Party Provider; or
3. the accuracy, availability, or reliability of any data, information, content, services, advice, or statements made available in connection with such Third-Party Offering.

B. **Representations and Warranties.** Customer represents and warrants that nothing in the Agreement, or Customer's use of Google Security Operations, will violate any agreement or terms with a third party to which Customer is subject.

ii. **Looker and BigQuery.** Google uses Looker and BigQuery with Google Security Operations for dashboarding, reporting, and storage features. Customer may only use Looker and BigQuery as part of Google Security Operations subject to any deployment, configuration, and use limitations provided or described by Google. Google may make Software available to Customer in connection with Customer's use of Looker, including third-party Software. Some Software may be subject to third-party license terms, which can be found at <https://looker.com/trust-center/legal/notices-and-acknowledgements>. If Customer stops using Google Security Operations, or Looker, then Customer

will also stop using the Software. Customer's access to Looker and/or BigQuery may be terminated by Google, at any time, if Customer is found to be in breach of the Agreement. Notwithstanding anything to the contrary in the Agreement, as used in this Section 1(d)(ii), the term "Customer Data" means (a) all data in Customer's databases provided to Looker by Customer or End Users via Google Security Operations, and (b) all results provided to Customer or End Users for queries executed against such data via Looker. Google's data location commitments under General Service Terms Section 1 (Data) do not apply to Looker or BigQuery dashboarding, reporting, or storage.

iii. *Google SecOps Enterprise Plus*. Google (Chronicle) Security Operations Enterprise Plus includes Google Threat Intelligence. If Customer subscribes to the SecOps Enterprise Plus SKU, as specified in an Order Form, then in addition to these Google Security Operations Service Terms, the Google Threat Intelligence and VirusTotal Service Terms in Section 3 also apply. For the avoidance of doubt, Google Threat Intelligence is not part of the Audited Services as set forth in the Cloud Data Processing Addendum, and Google's data location commitments under General Service Terms Section 1 (Data) do not apply to Google Threat Intelligence.

iv. *Google Unified Security*. If Customer subscribes to the Google Unified Security SKU, as specified in an Order Form, then in addition to the Agreement, including these Google Security Operations Service Terms, the following additional terms apply:

A. *GCP Service Entitlements*. Google Unified Security provides access to certain Google Cloud Platform services, namely Chrome Enterprise Premium, Security Command Center, and Web Risk (each as described in the Google Cloud Platform Services Summary (<https://cloud.google.com/terms/services?hl=en>)) (collectively, the "GCP Service Entitlements"). Customer's use of the GCP Service Entitlements is governed by Customer's agreement under which Google has agreed to provide Google Cloud Platform to Customer, including the Google Cloud Platform Service Specific Terms (<https://cloud.google.com/terms/service-terms>) (and, other than this subsection, these SecOps Service Specific Terms will not apply to the GCP Service Entitlements). For clarity, (i) the GCP Service Entitlements are Google Cloud Platform Services, and not SecOps Services, including for purposes of the Cloud Data Processing Addendum, and (ii) the applicable SLAs for the GCP Service Entitlements are published at <https://cloud.google.com/terms/sla>, to the exclusion of any SecOps Service SLAs referenced in the Agreement.

B. *Additional SecOps Entitlements*. Google Unified Security also includes Mandiant Threat Defense (a Mandiant Managed Services entitlement), Mandiant Retainer, and Google Threat Intelligence (collectively, the "Additional SecOps Entitlements"). Customer's use of the Additional SecOps Entitlements is governed by the specific terms applicable to each service included in these SecOps Service Terms. For clarity, Google Threat Intelligence and Mandiant Retainer are not considered Audited Services (as defined in the Cloud Data Processing Addendum), and the

data location commitments outlined in Section 1 (Data) of the General Service Terms do not apply to the Additional SecOps Entitlements.

e. *Service Limits*. Google may restrict a Customer's ingestion of data into Google Security Operations that exceed quotas ("Quotas"). Quotas are enforced to protect the community of Google Security Operations users by preventing unforeseen spikes in usage and overloaded services. Customer's Quota is specified in the Account. Additional information regarding Quotas can be found in the Documentation.

f. *Grounding with Google Search*. "Grounding with Google Search" is a Generative AI Feature of Google Security Operations that provides Grounded Results and Search Suggestions. "Grounded Results" mean responses that Google generates using the prompt from Customer, contextual information that Customer may provide (as applicable), and results from Google's search engine. "Search Suggestions" (also known as "Search Entry Points") mean search suggestions that Google provides with the Grounded Results. If a Grounded Result is clicked on, separate terms (not these terms) govern the destination page. If a Search Suggestion is clicked on, the Google Terms of Service (<https://policies.google.com/terms>) govern the google.com destination page. Grounded Results and Search Suggestions are generated output. "Links" are any means to fetch web pages (including hyperlinks and URLs) which may be contained in a Grounded Result or Search Suggestion. Links also include titles or labels provided with those means to fetch web pages. Excluding a Customer-owned web domain, Customer will not assert ownership rights in any intellectual property in Search Suggestions or Links in Grounded Results.

i. *Use Restrictions for Grounding with Google Search*. Customer:

A. Will only use Grounding with Google Search in connection with its use of Google Security Operations and in accordance with the Agreement.

Customer will only display the Grounded Results with the associated Search Suggestion(s) to the End User who submitted the prompt.

B. Will not, and will not allow its End Users or any third party to, store, cache, copy, frame, implement any click tracking, Link-tracking or other monitoring of (except as provided below), syndicate, resell, analyze, train on, or otherwise learn from Grounded Results or Search Suggestions.

C. Unless permitted by Google in writing (including in the Documentation), Customer:

1. will not modify, or intersperse any other content with, the Grounded Results or Search Suggestions; and

2. will not place any interstitial content between any Link or Search Suggestion and the associated destination page, redirect End Users away from destination pages, or minimize, remove, or otherwise inhibit the full and complete display of any destination page.

ii. *Storage for Debugging and Testing*. Customer acknowledges that it is reasonably necessary for Google to store prompts, contextual information that Customer may provide, and generated output for thirty (30) days for the purposes of creating Grounded Results and Search Suggestions, and since such information is being stored, Customer instructs Google that the stored information can be used for debugging and testing of systems that support Grounding with Google Search.

- iii. *Survival*. This subsection (f) (Grounding with Google Search) will survive termination or expiration of the Agreement, as applicable.
- g. *Grace Period and Renewal*.
 - i. *Grace Period*. If Customer continues to use Google Security Operations after the end of an Order Term without a written renewal agreement, then the subscription will automatically enter a grace period (each, a “Grace Period”). All usage during a Grace Period will be subject to the Agreement and at the then-current list prices. Google will invoice Customer (or the Reseller for usage by Resold Customers) monthly in arrears for such usage. For clarity, any discounts or credits previously agreed to will not apply to usage during a Grace Period.
 - ii. *Renewal*. If Customer renews its subscription during a Grace Period, the renewal will be governed by the terms of the new Order Form. If the new Order Form’s Services Start Date precedes its Effective Date, then (A) the renewal subscription will begin on the new Order Form’s Effective Date, and (B) Google will invoice Customer Grace Period fees for the period between the new Order Form’s Services Start Date and the new Order Form’s Effective Date, in accordance with subsection (i) above.
 - iii. *Grace Period Termination*. The Grace Period will terminate on the earlier of the renewal subscription start date or upon written notice by Google. If Customer does not timely renew its subscription during a Grace Period, then Google may, in its sole discretion, terminate the Grace Period and Customer’s access to Google Security Operations.
- h. *Additional Definitions*.
 - “*Covered Personnel*” means an employee or contractor of Customer.
 - “*Customer Network*” means the network used by Customer for internal business purposes, and all applications, software, services, and physical devices used for internal business purposes that connect to such network.
 - “*Data Cap*” means the amount of Customer Data that Customer is permitted to provide to Google Security Operations through the Account on an annual basis starting from the Service(s) Start Date, as specified in an Order Form as “Unit(s)”.
 - “*Data Limitation Notice Period*” means either (a) 72 hours after Google’s notice to Customer of non-compliance or (b) 7 days after Google’s notice if Customer reasonably demonstrates to Google that Customer is taking reasonable steps to remedy the non-compliance.
 - “*Data Period*” means the length of time that Customer Data will be available in Google Security Operations, as specified in an Order Form. The Data Period is calculated on a monthly rolling, lookback basis from the current date using the event date/timestamp of the Customer Data as read by Google Security Operations. If not specified in an Order Form, the Data Period is 12 months.
 - “*Documentation*” means the then-current Google Security Operations documentation made available by Google to its customers for use with the Services at <https://cloud.google.com/chronicle/docs>.
 - “*Generative AI Feature(s)*” has the meaning given in the General Service Terms above.
 - “*Network Telemetry*” means Security Telemetry generated by devices that are part of the Customer Network and does not include Security Telemetry generated by anyone or anything other than Covered Personnel; for example

Network Telemetry does not include Security Telemetry generated by Customer's customers or Customer's partners.

"*Security Telemetry*" means the metadata or other data that relates to Customer's or a Customer End User's security posture and that is produced by security related features, products, or services.

"*Third Party Telemetry*" means Security Telemetry Customer has received from a third party that Customer uses for purposes of securing the Customer Network.

"Units" means the units by which use of a Service SKU is measured (e.g., Data Cap or Covered Personnel).

2. Mandiant

a. Mandiant Solutions

i. Access to Mandiant Solutions. Subject to the Agreement, payment of all Fees, and any applicable Scope of Use, Customer may access and use the Mandiant Solutions specified in an Order Form in accordance with the Agreement and any Documentation, solely for its internal business purposes.

1. *Mandiant Security Validation*. Mandiant Security Validation may only be used up to the purchased license entitlement listed on the Order Form. Customers purchasing the Validation on Demand version of Mandiant Security Validation are licensed to use 1 actor to conduct 1 assessment, as set forth in the Documentation, and such use must occur within 1 year from the date of the applicable Order Form. The term of the license will begin on or shortly after the Order Form Effective Date (as determined by Google).

2. *Mandiant Attack Surface Management*. Customers may only use Mandiant Attack Surface Management up to the purchased license entitlements on the Order Form for the purpose of assessing the security of internet-facing assets in connection with Customer's business.

3. *Intelligence Subscriptions*. Customer may purchase different Intelligence Subscriptions, as set forth in the Documentation. Customer's access to the Intelligence Subscription(s) is provided through access keys or login credentials, which may not be shared between Customer's End Users. Customer may not establish group accounts. Google reserves the right to limit the number and/or frequency of requests through the Intelligence Subscriptions, as set forth in the Documentation. In addition to any other rights under the Agreement, Google may use technical measures to prevent over-usage or to stop usage after any limitations are exceeded.

4. *Mandiant Digital Threat Monitoring*. Customer may use Mandiant Digital Threat Monitoring solely for the purpose of analyzing Customer's own security posture and for no other purpose. Google may terminate or suspend Customer's usage of Mandiant Digital Threat Monitoring based on a suspected violation of this Section 2(a)(i)(5) (as determined in Google's sole discretion).

ii. Security Content.

1. *License*. Mandiant Solutions may include access to certain defined files, URLs, IP addresses, file hashes, commands, network traffic samples and other artifacts that can be malicious and/or represent real attacker behavior

("Security Content"). Google grants to Customer a limited, non-transferable, non-exclusive license to use the Security Content solely in connection with the applicable Mandiant Solutions and for no other purpose. Any Security Content obtained or licensed from a third party and furnished through Google or which Customer procures on its own will be deemed a Third Party Offering under the Agreement. Google does not warrant that any Security Content made available through Mandiant Solutions will continue to be available throughout the Order Term, and Google may add or remove Security Content from time to time in its sole discretion.

2. *Disclaimer.* Customer understands that Security Content includes live malware, including ransomware, and that use of the Security Content in ways not strictly described in the Documentation may cause damage to Customer's environment. Security Content is provided "as-is" and Google makes no representations or warranties regarding the Security Content and does not guarantee or warrant that the Security Content will cover all possible conditions, environments or controls. Security Content is obtained from a variety of sources, which may include known threat actors. To the maximum extent permitted by applicable law, Customer assumes all risk associated with use of the Security Content, and acknowledges that Google has no obligation to ensure Security Content will operate as intended.

3. *Submission of Security Content.* Mandiant Solutions may allow Customer to submit Security Content or other malware to Google. Customer acknowledges that any Security Content or other malware provided by Customer through the Mandiant Solutions is not Customer Data, and may be used, aggregated, analyzed and shared by Google to enhance the products and services Google provides to its customers.

b. Mandiant Managed Services

i. *Provision of Mandiant Managed Services.* During the Order Term, Google will provide Mandiant Managed Services as set forth in the Documentation, according to the volume of entitlements or licenses purchased by Customer set forth in the applicable Order Form. Any Mandiant Managed Services Customer requests that are not described in the Documentation will be performed at mutually agreed upon rates. If the number of entitlements or licenses exceeds the purchased volume reflected in the Order Form, Google will notify Customer in writing, and will issue an invoice for the next higher count at Google's then-current rates prorated for the remaining portion of the then-current Order Term. Google's data location commitments set out in these Service Specific Terms will not apply to Mandiant Managed Services.

ii. *Reseller and Partner Purchases.* If Customer receives Mandiant Managed Services via a Google authorized partner (a "Partner"), Customer agrees that the Mandiant Managed Services and any output of the Mandiant Managed Services, including reports, may be delivered to Customer through the Partner. Notwithstanding anything to the contrary in the Agreement, Customer authorizes Google to disclose information related to the Mandiant Managed Services and Customer Data to Partner.

iii. *Customer Responsibilities.* Customer acknowledges and agrees that (i) Mandiant Managed Services are not an alternative to an incident response engagement for an environment that is compromised prior to the start of the

Mandiant Managed Services Order Term, and (ii) Google's ability to successfully deliver the Mandiant Managed Services is dependent on the Customer's ability to meet its responsibilities as outlined in this Section 2(b)(iii). To the maximum extent permitted by applicable law, Google will have no liability for any failure to deliver the Mandiant Managed Services that may arise due to Customer's refusal or failure to perform its responsibilities:

1. *Installation Requirements.* Customer will be responsible for the following: (i) providing network architecture diagrams, physical, and logical access to Customer's environment for the sole purpose of deploying and configuring any Mandiant Managed Services supported technology (as may be defined in the Documentation); (ii) upgrading pre-existing technology to the minimum software version as referenced within the Documentation; (iii) providing confirmation that all technology within the Customer's environment has been successfully configured and connected to its network according to the individual product's system administration guide and the configurations supported as noted in the relevant product's support terms; and (iv) providing the ability to establish a persistent connection to the Customer's network within the designated port range corresponding to the country from which the Mandiant Managed Services will be delivered.
 2. *Credential Security.* Customer will be responsible for the following: (i) providing accurate information to Google for provisioning access to (and removal of) Customer personnel access to any portals associated with the Mandiant Managed Services; (ii) implementing and adhering to strong password standards; (iii) providing accurate information to Google for domain whitelisting; and (iv) reporting any security issues related to the Mandiant Managed Services (including any available portals) to Google immediately.
 3. *Network Segment Exclusion.* Customer will notify Google if specific network segments will not require managed defense monitoring. Customer must provide detailed information regarding the specific network segment range when possible (e.g. guest networks, testing environments).
 4. *Remediating Known Compromises.* Customer will make a reasonable effort to remediate any known compromises reported by Google or third party vendors. Google may choose to suppress alerts generated by known compromised systems until such time as the compromise is remediated.
 5. *Time and Date Settings.* Customers will ensure that all supported technology has accurate time and date settings, to help ensure that time-supported alerts are accurately categorized. Google will not be responsible for reporting on alerts generated by supported technology that does not have up to date time and date settings.
- iv. *Exclusions.* Notwithstanding anything to the contrary in the Agreement, Google will have no obligation to provide the Mandiant Managed Services for (i) products or services that have been declared end of support or that are not currently supported; (ii) products or services that have no active support in place; (iii) products or services for which updates have not been applied; (iv) products or services that have not been installed and deployed; or (v) products or services that are misconfigured or incorrectly deployed, which prevents the Mandiant Managed Services from monitoring. Customer

acknowledges that to facilitate Google's efficient performance of the Mandiant Managed Services, Google may control some features and functionality of the underlying products and services, including by applying updates, and such features or functionality may not be available for Customer's independent use during the Order Term of the Mandiant Managed Services.

c. Mandiant Consulting Services

- i. *Provision of Mandiant Consulting Services.* Google will provide the Mandiant Consulting Services specified in an Order Form, including Deliverables, to Customer, subject to Customer fulfilling its obligations under Section 2(c)(v) (Customer Obligations) below. Deliverables are considered final upon the earlier of Customer's written or oral confirmation of acceptance, or ten (10) business days after Google makes the Deliverables available to Customer.
- ii. *Invoices and Payment.* Customer will pay all Fees for Mandiant Consulting Services and some Fees may be non-cancellable, as specified in the Order Form.
- iii. *Personnel.* Google will determine which Personnel will perform the Mandiant Consulting Services. If Customer requests a change of Personnel and provides a reasonable and lawful basis for such request, then Google will use commercially reasonable efforts to replace the assigned Personnel with alternative Personnel. If provided to Google before the start of the Mandiant Consulting Services, Google's Personnel performing the Mandiant Consulting Services will comply with Customer's reasonable personnel training policies related to the Mandiant Consulting Services.
- iv. *Compliance with Customer's Onsite Policies and Procedures.* Google Personnel performing Mandiant Consulting Services at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.
- v. *Customer Obligations.*
 1. *Cooperation.* Customer will provide reasonable and timely cooperation in connection with Google's provision of the Mandiant Consulting Services. Google will not be responsible for a delay caused by Customer's failure to provide Google with the information, materials, consents, or access to Customer facilities, networks, systems, or key individuals required for Google to perform the Mandiant Consulting Services. If Google informs Customer of such failure and Customer does not cure the failure within 30 days, then Google may terminate any incomplete Mandiant Consulting Services and Customer will pay actual costs incurred by Google for the canceled Mandiant Consulting Services.
 2. *Expenses.*
 - a. *General.* Customer will reimburse expenses as specified in the applicable Order Form.
 - b. *Legal Expenses.* If Google (including its Affiliates and Personnel) is requested by Customer or receives Legal Process to produce information, documents or personnel as witnesses with respect to the Mandiant Consulting Services or the Agreement, Customer will reimburse Google (including its Affiliates and Personnel, as applicable)

for any time, expenses, and liabilities (including reasonable external and internal legal costs or fines and attorney's fees) incurred to respond to the request, unless Google (including its Affiliates and Personnel, as applicable) is itself a party to the proceeding or the subject of the investigation.

3. *Shipping Media.* Customer acknowledges and agrees that Google is not responsible for any damages arising from the shipment and delivery of any media, hardware, and equipment to Google.

4. *Information and Systems.* Customer is solely responsible for the accuracy and completeness of all information it and its Personnel provide to Google, and Customer represents and warrants that it owns, or is authorized to give Google access to, any systems, facilities, and/or devices that Google is required to access to perform the Mandiant Consulting Services.

vi. Intellectual Property.

1. *Background IP.* Customer owns all rights, title, and interest in Customer's Background IP. Google owns all rights, title, and interest in Google's Background IP. Customer grants Google a license to use Customer's Background IP to perform the Mandiant Consulting Services (with a right to sublicense to Google Affiliates and subcontractors). Except for the license rights under Sections 2(c)(vi)(2) (Google Technology) and 2(c)(vi)(3) (Deliverables) below, neither party will acquire any right, title, or interest in the other party's Background IP under the Agreement. For clarity, Background IP is included in the definition of "Indemnified Materials" for each party.

2. *Google Technology.* Google owns all rights, title, and interest in Google Technology. To the extent Google Technology is incorporated into Deliverables, Google grants Customer a limited, worldwide, non-exclusive, non-transferable license (with the right to sublicense to Affiliates), for the maximum term permitted by applicable law, to use the Google Technology in connection with the Deliverables for Customer's internal business purposes. The Agreement (including these Service Specific Terms) does not grant Customer any right to use materials, products, or services that are made available to Google customers under a separate agreement.

3. *Deliverables.* Google grants Customer a limited, worldwide, non-exclusive, fully-paid, non-transferable license (with the right to sublicense to Affiliates), for the maximum term permitted by applicable law, to use and reproduce the Deliverables for Customer's internal business purposes.

vii. Warranties and Remedies.

1. *Google Warranty.* Google will perform the Mandiant Consulting Services in a professional and workmanlike manner, in accordance with practices used by other service providers performing services similar to the Mandiant Consulting Services. Google will use Personnel with requisite skills, experience, and qualifications to perform the Mandiant Consulting Services.

2. *Remedies.* Google's entire liability and Customer's sole remedy for Google's failure to provide Mandiant Consulting Services that conform with Section 2(c)(vii)(1) (Google Warranty) will be for Google to, at its option,

(a) use commercially reasonable efforts to re-perform the Mandiant Consulting Services or (b) terminate the Order Form and refund any applicable Fees received for the nonconforming Mandiant Consulting Services. Any claim that Google has breached the warranty as described in Section 2(c)(vii)(1) (Google Warranty) must be made within 30 days following the date that Google has performed the applicable Mandiant Consulting Services.

viii. Indemnification.

1. *Indemnification Exclusions.* The sections of the Agreement titled “Google Indemnification Obligations” and “Customer Indemnification Obligations” will not apply to the extent the underlying allegation arises from (a) modifications to the Google Indemnified Materials or Customer Indemnified Materials (as applicable) by anyone other than the indemnifying party or (b) compliance with the indemnified party’s instructions, design, or request for customized features.

2. *Infringement Remedies.* The remedies described in the section of the Agreement titled “Remedies” also apply to Deliverables.

ix. *Survival.* The following Sections of these Mandiant Consulting Service Terms will survive expiration or termination of the Agreement or applicable Order Form: 2(c)(vi) (Intellectual Property), 2(c)(viii) (Indemnification), 2(c)(ix) (Survival), and 2(f) (Additional Definitions).

x. *Insurance.* During the term of the Agreement, each party will maintain, at its own expense, appropriate insurance coverage applicable to performance of the party’s respective obligations under the Agreement, including general commercial liability, workers’ compensation, automobile liability, and professional liability.

xi. *No Publicity.* Notwithstanding anything in the Agreement to the contrary, including the Agreement sections titled “Marketing and Publicity” and “Conflicting Terms”, neither party will publicly disclose that Google is providing Mandiant Consulting Services to Customer without the other party’s prior written consent in each instance.

xii. *Google Cloud Service Data.* If Customer also purchases Cloud Services (as defined in the Google Cloud Privacy Notice), then without limiting Google’s obligations under the Google Cloud Privacy Notice with respect to Service Data:

1. Google may access and process such data to provide Mandiant Consulting Services to Customer, as further described in the SecOps Privacy Notice; and
2. Customer will notify data subjects impacted by such processing as required by applicable law.

d. Mandiant Retainer (previously known as “Expertise On Demand”).

i. *Provision of Mandiant Retainer.* Google will provide Customer with the most current version of the Documentation that will describe the services available through the Mandiant Retainer Subscription (“Mandiant Retainer Services,” “Mandiant Retainer Subscription,” or “Mandiant Retainer”). Customer may order any of the Mandiant Consulting Services described in the Documentation during the twelve month period beginning on the Order

Form Effective Date (the “Covered Period”). All Services provided through Mandiant Retainer must commence within the Covered Period.

ii. *Retainer Units*. Customer will pay a fixed fee (the “Package Fixed Fee”) that entitles Customer to a specific number of Mandiant Retainer Units (“Retainer Units”), all as set forth on the applicable Order Form (“Unit Package”). The total Package Fixed Fee will be invoiced on or about the Order Form Effective Date. Each Mandiant Retainer Service will draw down the number of Retainer Units listed for that Service in the Documentation. Customer will make each request for Mandiant Retainer Services in writing as described in the Documentation. Customer may purchase additional Retainer Units (“Additional Units”) during the Covered Period. Retainer Units and Additional Units must be used during the Covered Period, and are non-cancelable and non-refundable. Retainer Units (including Additional Units) may not be used for any services not listed in the Documentation. Any technology fees and expenses will be invoiced separately as set forth in the Documentation. Retainer Units or Additional Units may be used to pay for such expenses. Any unused Retainer Units or unused Additional Units will expire if not drawn down during the Covered Period. Customer acknowledges and agrees that despite expiration of unused Retainer Units or Additional Units, Customer has received the benefit of the Mandiant Retainer Subscription.

iii. *Updates to Mandiant Retainer Services*. Customer acknowledges that Google may update the Documentation from time to time, and that the most current version of the Documentation will apply to the Mandiant Retainer Services. Notwithstanding the foregoing, Google will notify Customer at least twelve months in advance of discontinuing any Mandiant Consulting Service or increasing the number of Retainer Units required for any Mandiant Consulting Service.

iv. *Incident Response Service*. Subject to the terms governing Mandiant Consulting Services, Google will provide incident response services (“Incident Response Services”) during the Covered Period, as set forth in the Documentation. Incident Response Services may include:

1. Computer security incident response support.
2. Forensics, log and advanced malware analysis.
3. Advanced threat actor response support.
4. Advanced threat/incident remediation assistance.

v. *Additional Mandiant Service Terms*. If Customer orders Mandiant Consulting Services (including custom intelligence briefings) or Training Services as part of its Mandiant Retainer subscription, then Section 2(c) applies to Mandiant Consulting Services, and Section 2(e) applies to Training Services.

e. Training Services

i. *Provision of Training Services*. Customer may order Training Services subject to any Training Terms. The parties will mutually agree upon delivery dates and location for the Training Services specified in an Order Form. All Training Services (including rescheduled Training Services) must be scheduled and conducted within one year from the date of the Order Form

on which the applicable Training Services were purchased. Training Services do not include Deliverables.

1. *Private Training.* Customer will request rescheduling of private Training Services no less than two weeks in advance of the scheduled start date. Google will use reasonable efforts to reschedule Training Services, subject to availability, and Customer will pay any expenses associated with the rescheduling, including changing of travel plans. Customer may not record any aspect of the Training Services.
2. *Public Training.* If Customer cancels attendance at any public Training Services, Customer will notify Google no later than two (2) weeks before the date of the public Training Services, and Google will issue Customer a credit for the amount paid for the public Training Services. Customer will notify Google of any substitution of a named attendee for public Training Services. Google reserves the right to refuse admittance to public Training Services to any person, for any reason. If Google refuses admittance, Google will refund the amount paid for that person's public Training Services. Google does not refund or credit Fees paid for attendees who do not attend Training Services or who leave before Training Services conclude. Google reserves the right to cancel public Training Services and provide a refund for any reason. Customer may not record any aspect of the Training Services.
3. *On Demand Training.* On-demand Training Services must be completed within ninety days from the date of enrollment. Customer may not share or transfer access credentials for on-demand Training Services.

f. Additional Definitions.

"Background IP" means all Intellectual Property Rights owned or licensed by a party (a) before the effective date of the applicable Order Form or (b) independent of the Services.

"Deliverables" means written reports that are created specifically for Customer as a result of the Mandiant Consulting Services provided under the Agreement.

"Documentation" means the then-current Mandiant documentation made available by Google to its customers for use with the Services, as provided by Google upon Customer request.

"Google Cloud Privacy Notice" means the then-current Google Cloud Privacy Notice at <https://cloud.google.com/terms/cloud-privacy-notice>.

"Google Technology" means (a) Google Background IP; (b) all Intellectual Property and know-how applicable to Google products and services; (c) Indicators of Compromise; and (d) tools, code, algorithms, modules, materials, documentation, reports, and technology developed in connection with the Services that have general application to Google's other customers, including derivatives of and improvements to Google's Background IP. Google Technology does not include Customer Background IP or Customer Confidential Information.

"Indicators of Compromise" or "Indicators" means specifications of anomalies, configurations, or other conditions that Google can identify within an information technology infrastructure, used by Google in performing the Services.

“Order Form” means an order form, statement of work, or other document issued by Google under the Agreement, including data sheets associated with Services described in the order form, and executed by Customer and Google, specifying the Services Google will provide to Customer.

“Personnel” means a party’s and its Affiliates’ respective directors, officers, employees, agents, and subcontractors.

“SecOps Privacy Notice” means the then-current SecOps Privacy Notice at <https://cloud.google.com/terms/secops/privacy-notice>.

“Service Data” has the meaning given in the Google Cloud Privacy Notice.

“Training Terms” means the then-current terms applicable to Training Services provided to Customer by Google.

3. Google Threat Intelligence and VirusTotal (“GTI”)

a. Access and Use. Subject to the Agreement, payment of all Fees, and any applicable Scope of Use, Customer may access and use GTI as specified in an Order Form and Platform Security Content exclusively for Customer’s Internal Business Purposes. Customer’s access to its GTI Account is provided through access keys, including Google APIs, or login credentials, all of which Customer may not share with third-parties. Google reserves the right to limit the number and/or frequency of Customer’s requests through GTI, as set forth in the Documentation. In addition to any other rights under the Agreement, Google may use technical measures to prevent over-usage or to stop usage after any limitations are exceeded.

b. Restrictions. Except as otherwise expressly permitted in these GTI Service Terms, Customer will not, and will not allow End Users, including Customer Product End Users, to:

i. Sublicense, distribute, publicly perform or display, or otherwise share or make accessible, directly or indirectly, any Platform Security Content or results from GTI, including without limitation, any Google API or interface, or portions thereof, to any third party.

ii. Obtain or use any Platform Security Content except as specifically permitted, or use or attempt to use GTI to mine information in any way that could identify individual persons in their private capacity, attempt to access or misappropriate content contained in any Platform Security Content, or otherwise use GTI or Platform Security Content for any purpose other than to detect and prevent malware in a non-commercial personal or organizational capacity.

iii. Publicly attribute the Platform Security Content that Customer receives through GTI to any Security Partner (including, but not limited to any antivirus vendors, URL scanning engines, file characterization tools, etc.) without the individual Security Partner’s express written permission.

The restrictions contained in this subsection (b) are deemed to be “Restrictions” or “Use Restrictions” under the applicable Agreement.

c. Service Suspension. Google may Suspend Customer’s access to GTI if Customer does not comply with Section 3(a) (Access and Use) or Section 3(h)(ii)(C) of these GTI Service Terms, provided that Google will provide Customer notice of Suspension without undue delay, to the extent legally permitted.

d. Disclaimer. Customer understands that Platform Security Content includes live malware, including ransomware, and that use of Platform Security Content in ways not strictly described in the Documentation may cause damage to Customer's environment. Platform Security Content is provided "as-is" and Google makes no representations or warranties regarding Platform Security Content and does not guarantee or warrant that Platform Security Content will cover all possible conditions, environments or controls. Platform Security Content is obtained from a variety of sources, which may include known threat actors. To the maximum extent permitted by applicable law, Customer assumes all risk associated with the use of Platform Security Content, and acknowledges that Google has no obligation to ensure that Platform Security Content will operate as intended.

e. Customer Submitted Content and Community Content Guidelines.

i. Customer may provide Customer Submitted Content to Google. Customer acknowledges and agrees that Google may use, aggregate, analyze, and share Customer Submitted Content, including with Security Partners, for the purpose of improving Google's and its Security Partners' products and services. Customer confirms that (i) Customer Submitted Content complies with the Agreement and the SecOps Privacy Notice; and (ii) it is either the original owner of Customer Submitted Content or possesses all necessary rights and permissions to irrevocably contribute and share the Customer Submitted Content, and related information, including with the Community.

ii. Customer retains ownership of its original material within the Customer Submitted Content. However, to the maximum extent permitted by applicable law, by uploading or submitting Customer Submitted Content Customer grants Google (and those that Google works with) a worldwide, royalty free, perpetual, irrevocable and transferable license to use, edit, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute all content contained within Customer Submitted Content.

iii. CUSTOMER AGREES THAT IT WILL ONLY UPLOAD CUSTOMER SUBMITTED CONTENT THAT IT WISHES TO PUBLICLY SHARE AND THAT IN ANY CASE, CUSTOMER WILL NOT KNOWINGLY SUBMIT ANY CUSTOMER SUBMITTED CONTENT TO GTI THAT CONTAINS CONFIDENTIAL OR COMMERCIALY SENSITIVE DATA WITHOUT LAWFUL PERMISSION. CUSTOMER FURTHER AGREES THAT IT WILL NOT SUBMIT ANY CUSTOMER SUBMITTED CONTENT TO GTI THAT CONTAINS PERSONAL DATA.

iv. Although Google has no obligation to monitor the use of GTI, user content, or any Customer Submitted Content, Google may monitor GTI to detect and prevent fraudulent activity or violations of the Agreement and retains absolute discretion to remove Customer Submitted Content, material or users from GTI at any time and for any reason without notice. In order to promote the security of the Community and information sharing accountability, accounts and Customer Submitted Content contributed by the Community (for example, comments, posts, etc.) generally will not be removed from GTI, unless they are illegal, violate the lawful rights of an individual, serve any other unethical/malicious purpose, or otherwise violate the Agreement.

- v. IF CUSTOMER DOES NOT WANT TO PUBLICLY SHARE CUSTOMER SUBMITTED CONTENT IN THE MANNER SET OUT IN THE AGREEMENT OR IN THE SECOPS PRIVACY NOTICE, CUSTOMER WILL NOT SEND IT/CONTRIBUTE IT TO GTI AS THE SERVICE IS DESIGNED TO WORK THROUGH THE COLLECTIVE AGGREGATION AND SHARING OF THREAT-INTELLIGENCE WITH AND THROUGH THE COMMUNITY.
- vi. Private Scanning. If Customer subscribes to the Private Scanning SKU, as specified in an Order Form, then notwithstanding this Section 3(e), any Customer Submitted Content uploaded by Customer through the GTI Private Scanning feature (“Private Scanning”) will not be shared with other customers, Security Partners, or the Community, unless it is also uploaded to the standard GTI service in addition to Private Scanning.
- f. Discontinuation and Termination.
 - i. Notwithstanding anything to the contrary in the Agreement, Google may discontinue new services, features, or functionality without prior notice to Customer. Any new services, features, or functionality may be subject to additional terms communicated to Customer.
 - ii. Upon termination or expiration of the Agreement or the applicable Order Form, Customer will immediately delete all Platform Security Content, including from any cloud repositories, file directories, storage media, or any other location or instance where it may be stored, and not use or create products or services incorporating any remaining Platform Security Content.
- g. Browser Extension. If Customer accesses GTI through the Browser Extension, Google will collect information about how domain names Customer visits are resolved. Passive Domain Name System Information (“pDNS”) data consists of domain names that Customer’s browser requests, along with the IP address resolutions for such domain names. Google will make this pDNS data available through GTI to enable members of the Community to better detect malicious domains that might be hosted on a server (contacted on a given IP address) controlled by an attacker. Collected pDNS data is distinct from browsing history and is never tied to a user or used to identify an individual. Existing users of the Browser Extension will need to opt-in to share pDNS data with the Community. Users downloading the Browser Extension for the first time may opt-out of this collection in the Browser Extension settings.
- h. GTI Integration SKUs. In addition to these GTI Service Terms, the following additional terms apply with respect to the GTI Integration SKUs.
 - i. *Permitted Use*. During the Term, and notwithstanding the internal business purposes requirement in Section 3(a) of these GTI Service Terms, Customer may use Platform Security Content to enhance Customer Products, provided that (a) the Customer Products have material value independent of GTI; and (b) Customer complies with the Agreement.
 - ii. *Restrictions*. Customer will not:
 - A. Allow any third party, including Customer Product End Users, to access Customer’s GTI Account, Google APIs, or Platform Security Content, except for GTI Widget Data as expressly permitted in Section 3(h)(iv)(A) of these GTI Service Terms;
 - B. Use GTI or Platform Security Content in or to train any artificial intelligence models;

- C. Use GTI or Platform Security Content to develop, offer, support, or enhance Customer Products or any other products or services that are competitive with Google Security Operations or GTI; or
- D. Make any representations, warranties, or commitments concerning GTI or Platform Security Content.

The restrictions contained in this subsection (h)(ii) are deemed to be “Restrictions” or “Use Restrictions” under the applicable Agreement.

iii. *Requirements.* Customer will:

- A. Comply with the GTI Integration Documentation;
- B. Be solely responsible for technical support of its Customer Products; and
- C. Ensure that any sale of Customer Products is governed by an enforceable End User Agreement that will remain effective until the end of the applicable Order Term, unless the Agreement is terminated earlier. Without affecting any commitments made by Google to Customer under this Agreement, to the maximum extent permitted by applicable law, Google is not responsible for, and will have no liability to Customer or Customer Product End Users in relation to, (a) any End User Agreement, or (b) Customer’s provision, access, or use of GTI, the GTI Widget, or Platform Security Content to, or on behalf of, Customer Product End Users.

iv. GTI-INT-Advanced and GTI-INT-Custom SKUs. The following additional terms apply to the GTI-INT-Advanced and GTI-INT-Custom SKUs, unless others specified.

- A. *GTI Widget.* Notwithstanding Section 3(b)(i) of these GTI Service Terms, Customer may, using Google APIs, integrate the GTI Widget into Customer Products for the sole purpose of enhancing Customer End User Security Telemetry with GTI Widget Data. Customer may display GTI Widget Data solely in a visual manner to Customer Product End Users. Customer is responsible for any Customer Product End User access to the GTI Widget and use of GTI Widget Data. If Customer displays GTI Widget Data to Customer Product End Users, then Customer will include the statement “Enriched by Google Threat Intelligence” in a clear and visible manner.

- B. *Public Facing Materials.*

Customer may publish materials and collateral about Customer Products, including blogs, whitepapers, and sales materials (“Public Facing Materials”). All Public Facing Materials must include the statement “Enriched by Google Threat Intelligence” in a clear and visible manner and in accordance with Google branding guidance made available to Customer. Customer is solely responsible for ensuring that all Public Facing Materials comply with applicable laws, including data protection laws.

Notwithstanding Section 3(h)(iv)(B)(1), Customer may not publish any other information concerning Google or its products or services, including GTI, or use Google Brand Features without Google’s prior written consent. This includes publication in Public Facing Materials or any other medium.

C. *GTI-INT-Custom SKU*. Unless otherwise agreed in an Order Form, the following additional terms apply only to the GTI-INT-Custom SKU:

Reports.

a. *Required Information*. For each Reporting Period, Customer will provide Google with a report (each, a “Report”). Each Report will include, at a minimum, the following information solely for the purposes of Google invoicing and verifying Customer’s compliance with the Agreement:

- The number of active Customer Product End Users and the number of Assets managed by Customer;
- Customer’s revenue from the Customer Products; and
- To the extent permitted by applicable law, each Customer Product End User’s number of employees, industry, and location.

b. *Submission*. Each Report is due within 30 days after the end of the applicable Reporting Period. Each Report will cover the period starting the day after the previous Reporting Period ended and continuing through the end of the current Reporting Period.

c. *Acceptance*. Within ten (10) business days of its receipt of a Report, Google may dispute, in good faith, the accuracy of a Report. If disputed, Customer and Google will work in good faith to resolve the dispute, which will include Customer promptly responding to any reasonable inquiries from Google and, upon request, providing Google with documentation necessary to resolve the dispute. Once accepted by Google, the Report will be deemed accepted for that Reporting Period and Google waives any further right to dispute the accuracy of the Report.

d. *Expansion*. If Customer’s consumption exceeds the Units purchased during an Order Term (as evidenced by the Report(s)), then Google will notify Customer and the parties will execute an Order Form to reconcile the excess Units.

v. *Additional Customer Indemnification Obligations*. In addition to Customer’s indemnification obligations under the Agreement, Customer will defend Google and its Affiliates providing GTI and Platform Security Content and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from (a) the Customer Products; (b) Customer Submitted Content; and (c) Customer and Customer Product End User access to and use of Platform Security Content.

i. *VirusTotal Free Users*. The SLAs, Google’s indemnity obligations under the Agreement, and the Technical Support Service Guidelines do not apply to free users of VirusTotal. For VirusTotal free users only, the definition of “Services” in the Agreement is replaced with the following:

“Services” means the VirusTotal malware intelligence service and platform that leverages real threat intelligence contributed by a global community of users.

j. *VirusTotal Legacy Customers*. For customers that purchased VirusTotal from Chronicle LLC or Chronicle Security Ireland Limited only, the VirusTotal Enterprise Terms at https://go.chronicle.security/hubfs/vt_terms.pdf, or an offline variant of those terms if available, govern the purchase and use of VirusTotal instead of the Agreement.

k. Additional Definitions.

“*Assets*” means a physical or virtual hardware or software security device protected by the Customer Product(s).

“*Browser Extension*” means the browser extension described at <https://docs.virustotal.com/docs/browser-extensions>.

“*Community*” means a member of the public, an AV, scanning, sandbox or other Security Partners, security-minded organizations and other licensed users of the Service.

“*Customer Product End User(s)*” means a third party individual or entity that interacts with the Customer Product(s). Customer Product End User(s) may only use the Customer Product(s) to protect their own internal employees, data, systems, networks, applications, users, and processes.

“*Customer Product(s)*” means an offering that Customer enhances or produces using GTI, or as specified in an Order Form. Customer Product(s) does not include GTI.

“*Customer Submitted Content*” means security-related objects and artifacts, including executable and non-executable files uploaded to, scanned, or analyzed by GTI, including by tools on the Site by users of GTI, and associated metadata, comments and/or posts made available through GTI. For the avoidance of doubt, Customer Submitted Content is not Customer Data.

“*Documentation*” means the then-current documentation made available by Google to its customers for use with GTI, as described at <https://docs.virustotal.com> and <https://gtidocs.virustotal.com/>, and as otherwise provided by Google upon Customer request.

“*End User Agreement*” means an agreement between Customer and a Customer Product End User under which Customer sells or supplies Customer Product(s).

“*GTI Integration Documentation*” means the then-current documentation made available by Google to its customers for use with the GTI Integration SKUs, at <https://www.virustotal.com/go/gti-integration-skus-docs>.

“*GTI Integration SKUs*” means a GTI SKU (i) listed at <https://assets.virustotal.com/google-ti-integration-packages.pdf> as of the Order Form Effective Date; and (ii) ordered via (A) a signed Order Form directly from Google, or (B) a Reseller under a Reseller Agreement. For clarity, the GTI Integration SKUs include the GTI-INT-Core, GTI-INT-Advanced, and GTI-INT-Custom SKUs.

“*GTI Widget*” means a HTML widget that Customer integrates into Customer Products through a Google API and that enables Customer to display GTI Widget Data to Customer Product End Users.

“*GTI Widget Data*” has the meaning described in the GTI Integration Documentation and any summaries, derivative reporting, and metadata Customer derives from GTI Widget Data through its use of GTI.

“*Internal Business Purposes*” means protecting Customer’s internal employees, data, systems, networks, applications, users, and processes.

“*Platform Security Content*” means all content or data the Customer can interact with or retrieve from GTI, including files, URLs, IP addresses, domains, file hashes, commands, network traffic samples, Customer Submitted Content, GTI Widget Data, Google reporting, curated collections (including but not limited to actors, campaigns, malware, vulnerabilities), Google

attributions/associations on vulnerability objects, alerts/notifications, deep/dark web data, analyst comments and annotations, YARA signatures, and content/analysis related to tools techniques and procedures (TTPs), or threat profiles and other artifacts that can be malicious and/or represent real attack behavior.

“Reporting Period” means the interval of time covered by a Report, and the frequency with which Reports are due. For example, an annual Reporting Period means each Report will cover one year, and Reports will be due annually. For the first Report, the Reporting Period begins on the Order Form Effective Date. Google will notify Customer of the Reporting Period in writing unless otherwise defined in an Order Form. If not specified in writing by Google or in an Order Form, the Reporting Period is annual.

“Scope of Use” has the meaning given in the General Service Terms above.

“SecOps Privacy Notice” means the then-current SecOps Privacy Notice at <https://cloud.google.com/terms/secops/privacy-notice>.

“Security Partners” means members of the public, an antivirus, scanning, sandbox or other security partner who are using and contributing Customer Submitted Content to GTI.

“Security Telemetry” has the meaning given in the Google Security Operations Service Terms above. Security Telemetry only includes metadata or other data that is independently ingested into the Customer Product(s) not through GTI.

“Site” means the site located at [virustotal.com](https://www.virustotal.com) and all associated controlled and VirusTotal branded sites linked from [virustotal.com](https://www.virustotal.com) by Google and its Affiliates.

“Units” means the units by which use of a GTI Integration SKU is measured (e.g., Number of Customer Products).

4. Security Customer Success Services.

a. *Applicable Terms.* The terms in Sections 2(c) (Mandiant Consulting Services) and 2(f) (Additional Definitions) of these Service Terms, as amended in Section 4(b) below, apply to Security Customer Success Services.

b. *Amendments.* Sections 2(c) (Mandiant Consulting Services) and 2(f) (Additional Definitions) of these Service Terms are amended as follows with respect to Security Customer Success Services only:

i. References to “Mandiant Consulting Services” are each deemed to be references to “Security Customer Success Services”.

ii. Section 2(c)(i) (Provision of Mandiant Consulting Services) is modified to read as follows:

Provision of Security Customer Success Services. Google will provide the Security Customer Success Services specified in an Order Form, including Deliverables (if applicable), to Customer subject to Customer fulfilling its obligations under Section 2(c)(v) (Customer Obligations). Subject to the payment of all Fees, and any applicable Scope of Use, Customer may use Security Customer Success Services in accordance with the Agreement and any Documentation, solely for its internal business purposes. Any Deliverables are considered final upon the earlier of Customer’s written or oral confirmation of acceptance, or ten (10) business days after Google makes the Deliverables available to Customer. Security Customer Success Services do not include Training Services.

- iii. The following provisions in Section 2(c) do not apply to Security Customer Success Services and are deleted: Sections 2(c)(vii) (Warranties and Remedies); 2(c)(xi) (No Publicity); and 2(c)(xii) (Google Cloud Service Data).
- iv. The definition of Deliverables in Section 2(f) is modified to read as follows: “*Deliverables*” means work product provided to Customer by Google Personnel as part of the Security Customer Success Services and specified as Deliverables in an Order Form.

Partner-Specific Terms

1. Modification of Terms. The following amendments to these SecOps Service Specific Terms apply if the Agreement authorizes the resale or supply of SecOps Services under a Google Cloud partner or reseller program:

- (a) The Section titled “SecOps Specific Terms” of the terms posted here (<https://services.google.com/fh/files/misc/partner-authorization-terms.pdf>) (“SecOps Partner Authorization Terms”) apply to the resale or supply of the SecOps Services. Google may update the SecOps Partner Authorization Terms from time to time by posting any such update at the relevant URL page. Unless otherwise noted by Google, material updates to SecOps Partner Authorization terms will become effective 30 days after they are posted. Notwithstanding the preceding sentence, to the extent the updates are required by applicable law, the terms will be effective immediately.
- (b) The subsection of these SecOps Services Specific Terms under “Generative AI Features” titled “Restrictions” is amended to state: The restrictions contained in subsections (g) and (h) above are deemed to be additional restrictions in the “Use Restrictions” section under the applicable Agreement’s Google Cloud Platform Product Schedule.
- (c) Subsection (b) of these SecOps Service Specific Terms under “Google Threat Intelligence and VirusTotal (GTI)” is amended by deleting the last sentence of the subsection and replacing it with the following sentence: The restrictions contained in subsection (b) are deemed to be additional restrictions in the “Use Restrictions” section under the applicable Agreement’s Google Cloud Platform Product Schedule.
- (d) Subsection (h)(ii) of these SecOps Service Specific Terms under “Google Threat Intelligence and VirusTotal (GTI)” is amended by deleting the last sentence of the subsection and replacing it with the following sentence: The restrictions contained in subsection (h)(ii) are deemed to be additional restrictions in the “Use Restrictions” section under the applicable Agreement’s Google Cloud Platform Product Schedule.

2. Partner Software Terms. The following apply to Partner’s use of Software (including “Premium Software” as defined in the General Service Terms):

- (a) Sublicensing.
 - (i) Partner may sublicense Software, but only to its Customers who are obtaining the Software from Partner (“Authorized Sublicensees”).
 - (ii) Partner may not grant any Authorized Sublicensee the right to further sublicense any Software.
- (b) Provision Limitations. Unless Google has provided specific written instructions otherwise, Partner may not directly provide the Software to any third party (including any Authorized Sublicensee) and will instruct Authorized Sublicensees to directly download the Software from a URL or other repository provided by Google.

3. Partner-Licensed GTI Integration SKUs. If the Partner places an Order Form for GTI Integration SKUs in relation to a Partner’s Customer that is exempt as per the “Partner-Licensed Managed Security Services Customers” exemption as described at <https://cloud.google.com/terms/direct-tos-exemptions?e=48754805&hl=pt-br>, then:

- (a) Any references to “Customer Product(s)” is deemed a reference to “Partner Product(s)”, which means an offering that Partner enhances or produces using GTI, or as specified in an Order Form. Partner Product does not include GTI.
- (b) Any references to “Customer Product End User(s)” is deemed a reference to “Partner Product End User(s)”, which means a third party individual or entity that interacts with the Partner Product(s) and that may only use the Customer Product to protect its own internal employees, data, systems, networks, applications, users, and processes.
- (c) Any references to End User Agreement means an agreement between Partner and a Partner Product End User under which Partner sells or supplies Partner Products.



Google Cloud Platform Terms

Unless otherwise agreed in an Order Form or an amendment, the terms in this section apply when Google provides SecOps Services to Customer under a Google Cloud Platform Services Schedule to the Cloud Master Agreement or a Google Cloud Platform License Agreement (“GCPLA”) (collectively, the “GCP Terms”). In such instances, the terms in this Section form part of the GCP Terms and govern the provision and use of SecOps Services. For clarity, this Section does not apply to Google Cloud Platform Services.

1. **Modified Terms.** For SecOps Services only, the GCP Terms are modified as follows:

- a. The Section(s) titled “Accounts” and “Admin Console”, or “Account; Admin Console” is modified to read as follows:
Account. Google will provide Customer with the Account through which Customer may access the Services. Customer is responsible for (a) maintaining the confidentiality and security of the Account, associated passwords, and Google API keys, and (b) any use of the Account.
- b. The Section titled “Termination of Previous Agreements”, if applicable, is modified to read as follows:
Termination of Previous Agreements. If Google or a Google Affiliate and Customer have previously entered into a different agreement for the Services, then that agreement will terminate on the Services Start Date, and the Agreement will govern the provision and use of the Services going forward.
- c. The definition of “Account” is modified to read as follows:
“Account” means Customer’s SecOps Services account.
- d. The definition of “Customer Data” is modified to read as follows:
“Customer Data” means (i) data provided to Google by Customer or End Users through the Services under the Account and data that Customer or End Users derive from that data through their use of the SecOps Services, or (ii) for Mandiant Consulting Services and Managed Services only, data provided to Google by Customer or End Users in connection with receiving the Services.
- e. The definition of “Prices” is modified to read as follows:
“Prices” means the prices for the SecOps Services, Software, and Technical Support Services as described in an Order Form or amendment to the Services Schedule.

2. GCPLA Terms. In addition to the modifications in Section 1 (Modified Terms), the following additional modifications apply solely to SecOps Services purchased under a Google Cloud Platform License Agreement:

- a. The Section titled “Use of Customer Data” is modified to read as follows:
Use of Customer Data. Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. Google has implemented and will maintain technical, organizational, and



physical safeguards to protect Customer Data, as further described in the Cloud Data Processing Addendum.

- b. The Section titled “Usage and Invoicing” is modified to read as follows:
Usage and Invoicing. Customer will pay all Fees for the Services and TSS. Detailed usage data will be made available by Google to allow Customer to validate the Services purchased and associated Fees. Unless otherwise provided in the Agreement or required by law, Fees for Services are nonrefundable.

3. Non-Applicable GCP Terms. The following defined terms in the GCP Terms do not apply to SecOps Services: “Admin Console”, “Customer Application”, “Application”, “Documentation”, “Instance”, and “Project”.

4. Specific SecOps Terms. The following terms provide specific details and clarifications regarding the application of GCP Terms to SecOps Services:

- a. Data Location: Any “Data Location” provisions in the GCP Terms do not apply to SecOps Services. Instead, Section 1.b (Location) of the General Service Terms above governs data location for SecOps Services.
- b. Recovery Objectives (RTOs/RPOs): Any recovery time objectives or recovery point objectives (RTOs/RPOs) provided in the GCP Terms do not apply to SecOps Services.
- c. Compliance Certifications and SOC Reports: Notwithstanding any other provision in the GCP Terms regarding compliance certifications and reports, the certifications and reports that Google will maintain for SecOps Services are set forth at <https://cloud.google.com/security/compliance/secops/services-in-scope?hl=en>. Google may add standards at any time and may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.
- d. Cloud Data Processing Addendum: Google will process Customer Data in accordance with the Agreement, including the Cloud Data Processing Addendum.
- e. Service Level Agreements (SLAs): Unless explicitly stated otherwise, SLA commitments within the GCP Terms do not extend to SecOps Services.
- f. AI/ML Terms: Pursuant to the terms of the Agreement, SecOps Services are not Google Cloud Platform AI/ML Services and, therefore, unless explicitly stated otherwise, any “Artificial Intelligence” or “AI/ML” provisions in the GCP Terms do not apply to SecOps Services. Instead, Section 7 (Generative AI Features) of the General Service Terms above governs the use of AI functionalities within SecOps Services.
- g. Subprocessors and Subcontractors: Unless explicitly stated otherwise, any ‘Subprocessor’ or “Subcontractor” provisions in the GCP Terms do not apply to SecOps Services.

Previous versions (*Last modified January 1, 2026*)

December 11 2025, October 13 2025, September 4 2025, July 1 2025,
April 10 2025, January 30 2025, October 30 2024, September 5 2024,
July 15 2024, May 23 2024, April 4 2024, February 14 2024, September





19 2023, August 10 2023, June 15 2023, February 6 2023, October 31 2022, September 20 2021



Google Cloud Training Terms of Service

To receive the Training Services described below, Customer agrees to the terms of this Training Terms of Service (the "Agreement"). Together with an applicable Order Form, the Agreement governs Customer's receipt of Training Services from the Google entity referenced in the applicable Order Form.

1. Training Services Terms.

1.1 Training Services. After the parties complete and execute an Order Form: (a) Google will provide the Training Services to Customer and (b) Customer may use the Training Materials in accordance with this Agreement and as specified in an Order Form.

1.2 Instructor Led Training. Customer will provide reasonable access to appropriate facilities for Instructor Led Training provided at Customer's facilities.

1.3 Online Training. Google may offer Training Services or access to Training Materials online through Training Tools. Customer and Customer's End Users' use of Training Tools may be subject to separate use terms. Google is not responsible for Customer's inability to access Training Services on Training Tools due to Customer or Customer's End Users' violation of such use terms.

1.4 Use of Training Services. Customer must use Training Services within one (1) year of the applicable Order Form Effective Date. After one (1) year from the Order Form Effective Date, Google may (i) mark any unused Training Services as delivered; and (ii) if not already invoiced, invoice Customer for any unused Training Services on the Order Form. Customer will pay all Fees for Training Services on an Order Form unless an Order Form terminates for Google's material breach or either party's insolvency.

1.5 Rescheduling. Subject to Section 1.4 (Use of Training Services), Customer may reschedule Instructor Led Training up to two (2) times, on each occasion by canceling the Instructor Led Training with written notice more than 10 business days before the scheduled start date. After Customer has rescheduled two (2) times in accordance with the foregoing, then, unless otherwise agreed, Google may invoice Customer in full for any Fees not already invoiced for the Instructor Led Training and, if Fees are prepaid, mark the Training as delivered. If Customer cancels any Instructor Led Training 10 business days or less before the scheduled start date, or without written notice, Google may invoice Customer in full for Fees not already invoiced for the Instructor Led Training and, if Fees are prepaid, mark the Training as delivered.

1.6 Training Materials. Google will provide Training Materials to Customer's End Users in electronic or physical format. Unless otherwise authorized by Google, Customer may only share Training Materials with the number of End Users who have been authorized to receive Training Services under an Order Form. End Users may use Training Materials during the Term solely for the purpose of receiving the Training Services. Training Materials are Google Confidential Information and may not be shared with any unauthorized party. End Users may only use Training Materials provided through an online platform in connection with the End User's access to the platform.

1.7 Personnel. Google may offer Training Services, such as technical mentorship or program management, using Personnel. Google will determine which Personnel will



perform the Training Services. If Customer requests a change of Personnel and provides a reasonable and lawful basis for such request, Google will use commercially reasonable efforts to replace the assigned Personnel with alternative Personnel.

2. Customer Obligations.

2.1 Consents. Customer is responsible for any consents and notices required to permit Customer's and its End Users' use and receipt of the Training Services.

2.2 End User Equipment. Customer is responsible for ensuring End Users have access to appropriate equipment, facilities, and networks necessary to receive the Training Services and access the Training Materials.

2.3 Compliance. Customer will (a) ensure that Customer's and its End Users' use of the Training Services complies with the Agreement, (b) use commercially reasonable efforts to prevent and terminate any unauthorized access to or use of the Training Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Training Services of which Customer becomes aware.

2.4 Use Restrictions. Customer will not, and will not allow End Users or third parties under its control to: (a) copy, modify, or create a derivative work of the Training Services; (b) sell, resell, sublicense, transfer, or distribute the Training Services; (c) record the Training Services without Google's prior written consent; or (d) access or use the Training Services in a manner intended to avoid incurring Fees.

2.5 Cooperation. Customer will provide reasonable and timely cooperation in connection with Google's provision of the Training Services. Google will not be liable for a delay caused by Customer's failure to provide Google with information, equipment, consents or access to Customer facilities, networks or systems required for Google to perform the Training Services.

3. Payment Terms.

3.1 Payment. Google will invoice Customer for the Fees. Customer will pay all invoiced amounts by the Payment Due Date. All payments are due in the currency stated in the invoice. Wire transfer payments must include the bank information stated in the invoice. Unless required by applicable law, Fees for some Training Services may be non-cancellable, as specified on an Order Form.

3.2 Taxes. Customer is responsible for any Taxes, and will pay Google for the Services without any reduction for Taxes. If Google is obligated to collect or pay any Taxes, the Taxes will be invoiced to Customer and Customer will pay such Taxes to Google, unless Customer provides Google with a timely and valid tax exemption certificate in respect of those Taxes.

3.3 Invoice Disputes. Customer may dispute invoiced Fees if Customer believes in good faith that Fees were inaccurately invoiced (an "Invoice Dispute"). Invoice Disputes must be submitted to collections@google.com and identify all disputed amounts and the reasons for dispute. Google will review in good faith all Invoice Disputes, and will provide Customer an explanation of Fees due following such review (an "Invoice Dispute Report"). If an Invoice Dispute is submitted before the Payment Due Date, then notwithstanding Section 3.1 (Payment), (a) Customer must only pay the amounts not subject to the Invoice Dispute, and (b) unpaid Fees stated in an Invoice Dispute Report to be accurately invoiced are due within 30 days after delivery of such report. If an Invoice Dispute is submitted after the Payment Due



Date and the Invoice Dispute Report states that Fees paid were incorrectly invoiced, then Google will issue a credit equal to the agreed amount.

3.4 Overdue Payments.

a. If Customer's payment is overdue, except for amounts subject to an Invoice Dispute submitted before the Payment Due Date, then Google may (i) charge interest on overdue amounts at 1.5% per month (or the highest rate permitted by law, if less) from the Payment Due Date until paid in full, and (ii) Suspend the Training Services or terminate the applicable Order Form.

b. Customer will reimburse Google for all reasonable expenses (including attorneys' fees) incurred by Google in collecting overdue payments except where such payments are due to Google's billing inaccuracies.

3.5 Purchase Orders. If Customer requires a purchase order number on its invoice, Customer will provide a purchase order number in the Order Form. If Customer does not provide a purchase order number, then (a) Google will invoice Customer without a purchase order number, and (b) Customer will pay invoices without a purchase order number referenced. Any terms on a purchase order are void.

4. Intellectual Property.

4.1 Intellectual Property Rights. Except as expressly stated in Section 1.6 (Google Training Materials), the Agreement does not grant Customer any rights, implied or otherwise, to Google's Intellectual Property. Google retains all Intellectual Property Rights in the Training Services and Training Materials.

4.2 Feedback. At its option, Customer may provide feedback and suggestions about the Training Services to Google ("Feedback"). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer, excluding any Feedback marked as Customer Confidential Information.

5. Confidentiality.

5.1 Use and Disclosure of Confidential Information. The Recipient will only use the Disclosing Party's Confidential Information to exercise its rights and fulfill its obligations under the Agreement, and will use reasonable care to protect against the disclosure of the Disclosing Party's Confidential Information. Notwithstanding any other provision in the Agreement, the Recipient may disclose the Disclosing Party's Confidential Information (a) to its Delegates who have a need to know and who are bound by confidentiality obligations at least as protective as those in this Section 5 (Confidentiality); (b) with the Disclosing Party's written consent; or (c) subject to Section 5.2 (Legal Process), as strictly necessary to comply with Legal Process.

5.2 Legal Process. If the Recipient receives Legal Process for the Disclosing Party's Confidential Information, the Recipient will: (a) promptly notify the Disclosing Party prior to disclosure unless the Recipient is legally prohibited from doing so; (b) attempt to redirect the third party to request disclosure from the Disclosing Party directly; (c) comply with the Disclosing Party's reasonable requests to oppose disclosure of its Confidential Information; and (d) use commercially reasonable efforts to object to, or limit or modify, any Legal Process that the Recipient reasonably determines is overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. To facilitate the request in (b), the Recipient may provide the Disclosing Party's basic contact information to the third party. Notwithstanding



the foregoing, subsections (a) to (d) above will not apply in exceptional circumstances involving an imminent threat to life or risk of serious physical injury.

6. Representations and Warranties.

6.1 Each party represents and warrants that it has full power and authority to enter into the Agreement.

6.2 Anti-Bribery and Government Ethics Compliance. If the Training Services are being provided to a Customer who is a government entity, the Customer understands the Training Services can only be used for the benefit of the government entity and not by any individual government official for personal or hobby use. The Customer represents and warrants that (i) the Customer is authorized to accept the Training Services; (ii) acceptance of the Training Services is consistent with all applicable laws and regulations, including relevant anti-bribery and ethics rules and laws; and (iii) acceptance and use of the Training Services will not prevent Google from bidding on, or otherwise participating in, other potential contracts issued by the government entity or its related bodies. "Government entity" includes national, state, and local governments; government-owned or -controlled businesses or institutions (e.g., public universities, national telecom companies, etc.); public international organizations; political parties

7. **Disclaimer.** Except as expressly provided for in the Agreement, to the fullest extent permitted by applicable law, the Training Services and Training Materials are provided "as-is" and Google: (a) does not make any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, fitness for a particular use, noninfringement, or error-free or uninterrupted use of the Training Services or Training Materials; and (b) makes no representation about content or information accessible through the Training Services.

8. Liability.

8.1 Limited Liabilities

a. To the extent permitted by applicable law and subject to Section 8.2 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Agreement for any:

- (i) indirect, consequential, special, incidental, or punitive damages or
- (ii) lost revenues, profits, savings, or goodwill.

b. Each party's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the Fees Customer paid to Google under the applicable Order Form.

8.2 Unlimited Liabilities. Nothing in the Agreement excludes or limits either party's Liability for:

- a. death, personal injury, or tangible personal property damage resulting from its negligence or the negligence of its employees or agents;
- b. its fraud or fraudulent misrepresentation;
- c. its infringement of the other party's Intellectual Property Rights;
- d. its payment obligations under the Agreement; or
- e. matters for which liability cannot be excluded or limited under applicable law.

9. Term and Termination.



9.1 Agreement Term. The Agreement will remain in effect for the Term unless it expires or is terminated in accordance with the Agreement.

9.2 Termination for Convenience. Subject to any financial commitments in an Order Form or addendum to the Agreement, Customer may terminate the Agreement or an Order Form for any reason with 30 days' prior written notice to Google.

9.3 Termination for Breach.

a. Termination of an Order Form. Either party may terminate an Order Form if the other party is in material breach of the Order Form and fails to cure that breach within 30 days after receipt of written notice.

b. Termination of All Order Forms. Either party may terminate all effective Order Forms under the Agreement if the other party: (a) is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written notice; (b) ceases its business operations; or (c) to the extent permitted by applicable law, becomes subject to insolvency proceedings and such proceedings are not dismissed within 90 days.

9.4 Effects of Termination. Except as described in Section 9.3(b) (Termination of All Order Forms), the termination or expiration of one Order Form will not affect other Order Forms. If an Order Form terminates or expires, then:

a. Effect on Training Services. The rights under the Agreement granted by one party to the other regarding the Training Services will cease immediately except as described in this Section 9.4 (Effects of Termination); and Google will stop work on the Training Services; and

b. Effect on Payment. Customer will pay for: (i) Training Services, including work-in-progress, performed before the effective date of termination or expiration and (ii) any remaining non-cancellable Fees. Google will send Customer a final invoice for payment obligations under the Order Form.

c. Survival. The following Sections will survive expiration or termination of the Agreement: Section 3 (Payment Terms), Section 4 (Intellectual Property), Section 5 (Confidentiality), Section 7 (Disclaimer), Section 8 (Liability), Section 9.4 (Effects of Termination), Section 10 (Miscellaneous), and Section 11 (Definitions).

10. Miscellaneous.

10.1 Notices. Google will provide notice to Customer by sending an email to the Notification Email Address. Customer will provide notice to Google by sending an email to legal-notices@google.com. Notice will be treated as received when the email is sent. Customer is responsible for keeping its Notification Email Address current throughout the Term.

10.2 Emails. Under this Agreement, the parties may use emails to satisfy written approval and consent requirements.

10.3 Assignment. Neither party may assign the Agreement without the written consent of the other, except to an Affiliate where: (a) the assignee has agreed in writing to be bound by the terms of the Agreement, (b) the assigning party has notified the other party of the assignment, and (c) if Customer is the assigning party, the assignee is established in the same country as Customer. Any other attempt to assign is void.

10.4 Change of Control. If a party experiences a change of Control other than an internal restructuring or reorganization, then: (a) that party will give written notice to the other party within 30 days after the change of Control; and (b) the other party



may immediately terminate the Agreement any time within 30 days after it receives that written notice.

10.5 Force Majeure. Neither party will be liable for failure or delay in performance of its obligations to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, pandemics, terrorism, riots, or war.

10.6 Subcontracting. Google may subcontract obligations under the Agreement but will remain liable to Customer for any subcontracted obligations.

10.7 No Agency. The Agreement does not create any agency, partnership, or joint venture between the parties.

10.8 No Waiver. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Agreement.

10.9 Severability. If part of the Agreement is invalid, illegal, or unenforceable, the rest of the Agreement will remain in effect.

10.10 No Third-Party Beneficiaries. The Agreement does not confer any rights or benefits to any third party unless it expressly states that it does.

10.11 Equitable Relief. Nothing in the Agreement will limit either party's ability to seek equitable relief.

10.12 US Governing Law.

(a) For U.S. City, County, and State Government Entities. If Customer is a U.S. city, county, or state government entity, then the Agreement will be silent regarding governing law and venue.

(b) For U.S. Federal Government Entities. If Customer is a U.S. federal government entity, then the following applies: ALL CLAIMS ARISING OUT OF OR RELATING TO THE AGREEMENT OR THE SERVICES WILL BE GOVERNED BY THE LAWS OF THE UNITED STATES OF AMERICA, EXCLUDING ITS CONFLICT OF LAWS RULES. SOLELY TO THE EXTENT PERMITTED BY FEDERAL LAW, (I) THE LAWS OF THE STATE OF CALIFORNIA (EXCLUDING CALIFORNIA'S CONFLICT OF LAWS RULES) WILL APPLY IN THE ABSENCE OF APPLICABLE FEDERAL LAW; AND (II) FOR ALL CLAIMS ARISING OUT OF OR RELATING TO THE AGREEMENT OR THE SERVICES, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

(c) For All Other Entities. If Customer is any entity not identified in Section 10.12(a) (U.S. Governing Law for U.S. City, County, and State Government Entities) or (b) (U.S. Governing Law for Federal Government Entities), then the following applies: ALL CLAIMS ARISING OUT OF OR RELATING TO THE AGREEMENT OR THE SERVICES WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING THAT STATE'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA; THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

10.13 Amendments. Except as specifically stated otherwise in the Agreement, any amendment to the Agreement must be in writing, expressly state that it is amending the Agreement, and be signed by both parties.

10.14 Independent Development. Nothing in the Agreement will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs, or technology that are similar to the subject of the Agreement, provided that the party does not breach its obligations under the Agreement in doing so.



10.15 Entire Agreement. The Agreement states all terms agreed between the parties, and supersedes any prior or contemporaneous agreements between the parties, relating to the subject matter of this Agreement. In entering into the Agreement, neither party has relied on, and neither party will have any right or remedy based on, any statement, representation, or warranty (whether made negligently or innocently), except those expressly stated in the Agreement. Except as expressly provided for in the Agreement, nothing in the Agreement grants any right for Customer to use materials, products or services that are made available to Google customers under a separate license or agreement.

10.16 Conflicting Terms. If there is a conflict among the documents that make up the Agreement, then the documents will control in the following order (of decreasing precedence): the applicable Order Form and the Agreement.

10.17 Conflicting Languages; Currencies. If the Agreement is translated into any other language, and there is a discrepancy between the English text and the translated text, the English text will control. Unless otherwise specified, all references to "\$" in the Agreement refer to United States dollars.

10.18 Counterparts. The parties may execute the Agreement in counterparts, including facsimile, PDF, and other electronic copies, which taken together will constitute one instrument.

10.19 Electronic Signatures. The parties consent to electronic signatures.

10.20 Headers. Headings and captions used in the Agreement are for reference purposes only and will not have any effect on the interpretation of the Agreement.

11. Definitions.

"Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.

"Confidential Information" means information that one party (or an Affiliate) ("Disclosing Party") discloses to the other party ("Recipient") under or in connection with the Agreement, and that is marked as confidential or would normally be considered confidential information under the circumstances. Confidential Information does not include information that is independently developed by the Recipient, is shared with the Recipient by a third party without confidentiality obligations, or is or becomes public through no fault of the Recipient.

"Control" means control of greater than 50% of the voting rights or equity interests of a party.

"Customer" means the entity purchasing Training Services from Google as identified on an applicable Order Form.

"Delegates" means the Recipient's and its Affiliates' respective employees, agents, subcontractors, and professional advisors.

"Effective Date" means the date of the last party's signature on an Order Form incorporating the Agreement.

"End User" means an individual that Customer enables or permits to receive the Training Services under this Agreement. For clarity, End Users may include employees of Customer Affiliates and other authorized third parties.

"Fees" means the applicable fees for the Training Services stated on the applicable Order Form.

"Google" means the Google entity identified in the applicable Order Form.

"including" means including but not limited to.



"Instructor Led Training" means Training Services delivered as live instruction by Google or third party personnel. Instructor Led Training may be delivered in person or remotely.

"Intellectual Property" means anything protectable by an Intellectual Property Right.

"Intellectual Property Right(s)" means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

"Legal Process" means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure, or similar process.

"Liability" means any liability, whether under contract, tort (including negligence), or otherwise, regardless of whether foreseeable or contemplated by the parties.

"Notification Email Address" means the email address(es) designated by Customer in the applicable Order Form.

"Order Form" means an order form or other ordering document issued by Google, including data sheets associated with Services described in the Order Form, and executed by Customer and Google specifying the Training Services Google will provide to Customer.

"Payment Due Date" means 30 days from the invoice date in the applicable Order Form.

"Personnel" means Google's and Google's Affiliates' employees and subcontractors.

"Suspend" or "Suspension" means disabling access to or use of the Training Services or components of the Training Services.

"Taxes" means all government-imposed taxes, except for taxes based on Google's net income, net worth, asset value, property value, or employment.

"Term" means the period starting on the Effective Date and continuing until the earlier of termination, expiration or completion of the provision of Training Services under an Order Form.

"Training Materials" means courseware, materials or content made available to Customer by Google or third parties on behalf of Google for use in connection with the Training Services.

"Training Services" means education and training services for individuals or groups of users related to Google Cloud products and services, as more fully described in an applicable Order Form.

"Training Tools" means Google or third party platforms or communication tools, such as online forums, email or video conferencing.

12. Regional Terms. Customer agrees to the following modifications to the Agreement if Customer's billing address is in the applicable region as described below:

Asia Pacific - Australia

A new Section 7A is added as follows:

7A. This Section 7A applies only if the Services are subject to statutory guarantees under the Australian Competition and Consumer Act 2010 ("ACCA"). Applicable laws, including the ACCA, may confer rights and remedies into this Agreement that cannot be excluded, and which are not excluded by this Agreement. To the extent that the applicable laws permit Google to limit their operation, Google's and its



Affiliates' liability under those laws will be limited at its option, to the supply of the Services again, or payment of the cost of having the Services supplied again.

Section 8.1(b) (Limited Liability) is replaced with the following:

b. Google's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the greater of: (a) Fees Customer paid to Google under the applicable Order Form, and (b) \$AUD1000.

Section 10.12 (Governing Law) is amended by inserting the following text at the end of that Section: "If applicable law prevents a dispute from being resolved in a California court, then Customer may file the dispute in Customer's local courts. If applicable law prevents Customer's local court from applying California law to resolve a dispute, then the dispute will be governed by the applicable local laws of Customer's country, state, or other place of residence."

Section 10.15 (Entire Agreement) is amended by inserting the following text at the end of that Section: "Nothing in this Agreement excludes a party's liability for prior written or oral misrepresentation."

Latin America - Brazil

When the Google contracting entity is Google Cloud Brasil Computação e Serviços de Dados Ltda., Section 15.12 (U.S. Governing Law) is replaced as follows:

15.12 Governing Law & Arbitration. This Agreement is governed by Brazilian Law. ALL DISPUTES ARISING OUT OF OR RELATING TO THIS AGREEMENT OR ANY RELATED GOOGLE PRODUCTS OR SERVICES WILL BE SETTLED BY ARBITRATION, AS DESCRIBED BELOW.

(a) *Definitions.* "Dispute" means any contractual or non-contractual dispute regarding this Agreement, including its formation, validity, subject matter, interpretation, performance, or termination.

(b) *Settlement.* The parties will try in good faith to settle any Dispute within 30 days after a party receives the first notice regarding the Dispute in accordance with Section 15.12 (Notices). If the parties are unable to resolve the Dispute within this 30-day period, either party may refer the Dispute to arbitration in accordance with Section 15.12(c) (Arbitration).

(c) *Arbitration.* The parties will refer all Disputes to final, binding arbitration under the rules of the Center of Arbitration and Mediation of the Brazil-Canada Chamber of Commerce in force as of this Agreement's Effective Date ("Rules"). The arbitration will be conducted in Portuguese by three arbitrators in São Paulo, SP, Brazil, which will be the seat of arbitration.

(d) *Confidentiality.* The arbitration is Confidential Information (including the arbitration's existence and any oral or written information related to it). However, the parties may disclose to a competent court information necessary to execute any arbitral decision, but only if the confidentiality of those materials is maintained in those judicial proceedings.

(e) *Non-Monetary Relief.* The arbitrator(s) may only issue its award based on law, not in equity, and may not award non-monetary relief.

(f) *Fees and Expenses.* Each party will bear its own lawyers' and experts' fees and expenses, regardless of the arbitrator's final decision regarding the Dispute.

Latin America - Mexico

Section 3.2 (Taxes) is replaced as follows:

3.2 Taxes.



(a) Tax Invoicing and Payments. Taxes are not included in the Fees and will be separately itemized on Google's invoices if applicable. Customer will pay correctly-invoiced Taxes unless Customer provides a valid tax exemption certificate. If Customer is required by law to withhold any Taxes from its payments to Google, Customer must provide Google with an official tax receipt or other appropriate documentation to support such withholding.

(b) Tax Documentation. Google will timely provide customary tax documentation reasonably requested by Customer and vice versa.

Subsection b. in Section 8.1 (Limited Liabilities) is replaced as follows:

8.1 Limited Liabilities

a. [...]

b. To the extent permitted by applicable law, Google's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the Fees Customer paid to Google under the applicable Order Form.

Subsection a. of Section 8.2 (Unlimited Liabilities) is replaced as follows:

a. death, personal injury, or tangible personal property damage resulting from its gross negligence or the gross negligence of its employees or agents;

Section 10.12 (Governing Law) is replaced as follows:

10.12 Governing Law & Arbitration.

a. Governing Law. This Agreement is governed by the laws of the United Mexican States, excluding choice of law rules.

b. Arbitration.

(i) Definitions. "Dispute" means any contractual or non-contractual dispute regarding this Agreement, including its formation, validity, subject matter, interpretation, performance, or termination.

(ii) Settlement. The parties will try in good faith to settle any Dispute within 30 days after a party receives the first notice regarding the Dispute in accordance with Section 10.1 (Notices). If the parties are unable to resolve the Dispute within this 30-day period, either party may refer the Dispute to arbitration in accordance with Section 10.12 (iii) (Arbitration).

(iii) Arbitration. Except as prohibited by applicable law, the parties will refer all Disputes to final, binding arbitration under the Arbitration Rules of the National Chamber of Commerce of Mexico City in force as of this Agreement's Effective Date ("Rules"). The arbitration will be conducted in Spanish by one arbitrator, in Mexico City, Mexico, which will be the seat of arbitration.

(iv) Confidentiality. The arbitration is Confidential Information (including the arbitration's existence and any oral or written information related to it). However, the parties may disclose to a competent court information necessary to (a) require the aid of the competent courts before or during the arbitral proceeding; or (b) execute any arbitral decision, but only if the confidentiality of those materials is maintained in those judicial proceedings.

(v) Non-Monetary Relief. The arbitrator may only issue its award based on law, not in equity, and may not award non-monetary relief.

(vi) Fees and Expenses. Each party will bear its own lawyers' and experts' fees and expenses, and the arbitrator's final decisión must not include any rulings in this regard.

10.19 Electronic Signatures. The Parties expressly agree to execute this Agreement electronically and acknowledge that electronic signatures hold the same legal validity and enforceability as handwritten signatures, as recognized by applicable law. The





Parties further confirm that the electronic signatures used ensure the reliability, integrity, and inalterability of the document, binding the signature to the Agreement in accordance with applicable law. Each Party is responsible for safeguarding the security of its signature credentials, and the electronically signed Agreement shall be deemed final, complete, and binding.

The definition of "Taxes" under section 11 (Definitions) is replaced as follows:

11. Definitions

"Taxes" means all government-imposed tax obligations (including taxes, duties, and withholdings), except those based on net income, net worth, asset value, property value, or employment.

Previous versions (*Last modified September 11, 2025*)

June 19 2025, January 30 2025, October 16 2024, November 16 2023, February 16 2023, September 13 2022, March 29 2021

