Google Cloud Master Agreement – Public Sector
(Partner)

This Google Cloud Master Agreement is comprised of the Google Cloud Master Agreement General Terms ("General Terms"), and all Services Schedules that are each attached hereto and incorporated into the Google Cloud Master Agreement (collectively, the "Agreement").

Google Cloud Master Agreement General Terms

1. Services. After the Customer and Reseller and/or Distributor complete and execute an Order Form incorporating this Agreement, Google will provide the Services specified in the Order Form in accordance with the Agreement, including the SLAs, and Customer and its End Users may use the Services in accordance with the Services Schedule.

2. Customer Obligations.

2.1. Consents. Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Services and (b) Google's accessing, storing, and processing of data provided by Customer (including Customer Data, if applicable) under the Agreement.

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

2.3. Use Restrictions. Customer will not, and will not allow End Users to, (a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any of the source code of, the Services (except to the extent such restriction is expressly prohibited by applicable law); (b) sell, resell, sublicense, transfer, or distribute the Services; or (c) access or use the Services (i) for High Risk Activities; (ii) in a manner intended to avoid incurring Fees; (iii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (iv) in a manner that breaches, or causes the breach of, Export Control Laws; or (v) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA with Google (if approved), or an executed HIPAA BAA with Google's Reseller or Distributor.

3. RESERVED

4. Intellectual Property.

4.1. Intellectual Property Rights. Except as expressly described in the Agreement, the Agreement does not grant either party any rights, implied or otherwise, to the other's content or Intellectual Property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data and Customer Applications, and Google retains all Intellectual Property Rights in the Services and Software.

4.2. 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. 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 such disclosure unless the Recipient is legally prohibited from doing so; (b) attempt to redirect the third party to request it 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. Google acknowledges that the Customer may be subject to and must comply with the Freedom of Information Act (FOIA) or similar Open Records/Sunshine law.

6. Marketing and Publicity. Customer may state publicly that it is a Google customer and display Google Brand Features in accordance with the Trademark Guidelines. Google may use Customer's name and Brand Features in online or offline promotional materials of the Services. Each party may use the other party's Brand Features only as permitted in the Agreement. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features.

7. RESERVED.

8. Disclaimer. Google warrants that the Services or Software will, for a period of sixty (60) days from the date of your receipt, perform substantially in accordance with Services or Software written materials accompanying it. Except as expressly provided for in the Agreement (e.g. the SLA's as described in the definitions section), to the fullest extent permitted by applicable law, 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 Services or Software and (b) makes no representation about content or information accessible through the Services.

9. Indemnification.

9.1. Google Indemnification Obligations. Google will have the right to intervene to defend Customer and its Covered Affiliates, and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that the Google Indemnified Materials used in accordance with the Agreement infringe the third party's Intellectual Property Rights. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

9.2. Customer Indemnification Obligations. Subject to applicable federal or state law including GSA Schedule Contract Clause 552.212-4(u), and without waiving sovereign immunity, Customer will defend Google and its Affiliates providing the Services and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from (a) any Customer Indemnified Materials or (b) Customer's or an End User's use of the Services in breach of the AUP or the Use Restrictions. This section will not apply if the Customer is prohibited from agreeing to any vendor indemnification requirement.

9.3. Indemnification Exclusions. Sections 9.1 (Google Indemnification Obligations) and 9.2 (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) a combination of the Google Indemnified Materials or Customer Indemnified Materials (as applicable) with materials not provided by the indemnifying party under the Agreement, unless the combination is required by the Agreement.

9.4. Indemnification Conditions. Sections 9.1 (Google Indemnification Obligations) and 9.2 (Customer Indemnification Obligations) are conditioned on the following:

(a) Any indemnified party must 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 9.4(a) prejudices the defense of the Third-Party Legal Proceeding, the indemnifying party's obligations under Section 9.1 (Google Indemnification Obligations) or 9.2 (Customer Indemnification Obligations) (as applicable) will be reduced in proportion to the prejudice.

(b) Any indemnified party must 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.

9.5 Remedies.

(a) If Google reasonably believes the Services 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, (ii) modify the Services to make them non-infringing without materially reducing their functionality, or (iii) replace the Services with a non-infringing, functionally equivalent alternative.

(b) If Google does not believe the remedies in Section 9.5(a) are commercially reasonable, then Google may Suspend or terminate the impacted Services. If Google terminates Services under this Section 9.5 (Remedies), then upon Customer request (i) Google will refund to Customer any unused prepaid Fees that Customer paid to Google for use of the terminated Services, and (ii) if Customer has made financial commitments in an Order Form or addendum to the Agreement, then Google will agree to amend such commitments proportional to Customer's spend on the terminated Services in the year preceding the termination of the Services. For Federal Customers, if Google does not believe the remedies in Section 9.5(a) are commercially reasonable, the parties recognize that the provisions of 28 U.S.C.§ 1498 will apply to the resolution of any patent or copyright claim made by the patent or copyright owner.

9.6 Sole Rights and Obligations. Without affecting either party's termination or Suspension rights, this Section 9 (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 9 (Indemnification).

10. Liability.

10.1 Limited Liabilities.

(a) To the extent permitted by applicable law and subject to Section 10.2 (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 applicable Services Schedule during the 12 month period before the event giving rise to Liability.

10.2 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 9 (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.

11. Term and Termination.

11.1 Agreement Term. The Agreement, unless it expires or terminates according to the Reseller Agreement or Distributor Agreement, will remain in effect for the contract period as described in the applicable Reseller Agreement or Distributor Agreement (the "Term").

11.2 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 convenience with 30 days' prior written notice to Reseller or Distributor.

11.3 RESERVED.

11.4 Effects of Termination. If the Agreement terminates, then all Services Schedules and Order Forms also terminate. If an Order Form terminates or expires, then after that Order Form's termination or expiration effective date, (a) all rights and access to the Services under that Order Form will terminate (including access to Customer Data, if applicable), unless otherwise described in the applicable Services Schedule, and (b) Reseller or Distributor will send Customer a final invoice (if applicable) for payment obligations under that Order Form. Termination or expiration of one Order Form will not affect other Order Forms.

11.5 Survival. The following Sections will survive expiration or termination of the Agreement: Section 4 (Intellectual Property), Section 5 (Confidentiality), Section 8 (Disclaimer), Section 9 (Indemnification), Section 10 (Liability), Section 11 (Term and Termination), Section 12 (Miscellaneous), Section 13 (Definitions), and any additional sections specified in the applicable Services Schedule.

12. Miscellaneous.

12.1 Notices. Under the Agreement, notices to Customer must be sent to the Notification Email Address and notices to Google must be sent 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.

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

12.3 RESERVED.

12.4 RESERVED.

12.5 Force Majeure. In accordance with GSA Schedule Contract Clause 552.212-4(f), 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.

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

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

12.8 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.

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

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

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

12.12 RESERVED.

12.13 Amendments. Except as specifically described 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 Customer and Reseller.

12.14 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.

12.15 URL Terms. The URL Terms are incorporated by reference into the Agreement.

12.16 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 Data Processing Addendum, the applicable Services Schedule, the General Terms, and the other URL Terms.

12.17 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.

12.18 RESERVED.

12.19 RESERVED.

12.20 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.

12.21 Federal Customers. The Services were developed solely at private expense and are "commercial services," "commercial items," "commercial computer software," and "commercial computer software documentation," as those terms are defined within Section 2.101 of the Federal Acquisition Regulation ("FAR") and any applicable agency supplements to the FAR.

13. Definitions.

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

"AUP" means Google's acceptable use policy as defined in the applicable Services Schedule (if applicable).

"BAA" or "Business Associate Agreement " is an amendment to the Customer's Reseller Agreement or Distributor Agreement, or an executed HIPAA BAA with Google (if approved) covering the handling of Protected Health Information (as defined in HIPAA).

“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 its Affiliate (“Disclosing Party”) discloses to the other party (“Recipient”) under the Agreement, and that is marked as confidential or would normally be considered confidential information under the circumstances. Customer Data is Customer’s Confidential Information. 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.

“Covered Affiliate” has the meaning described in the Services Schedule (if applicable).

“Customer” means the party executing an Order Form with a Reseller for Google Services as described in the Agreement.

“Customer Application” has the meaning described in the Services Schedule (if applicable).

“Customer Data” has the meaning described in the Services Schedule (if applicable).

“Customer Indemnified Materials” has the meaning described in the applicable Services Schedule.

“Delegates” means the Recipient’s employees, Affiliates, agents, or professional advisors.

“Distributor” means an entity authorized by Google to distribute the Services to a Reseller for resale to federal, state, or local government entities of the United States (or representatives of such entities).

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

“Effective Date” means the date of the last party’s signature of the General Terms (or other applicable ordering document that incorporates the General Terms).

“End User” or “Customer End User” has the meaning described in the Services Schedule (if applicable).

“Export Control Laws” means all applicable export and re-export control laws and regulations, including (a) the Export Administration Regulations (“EAR”) maintained by the U.S. Department of Commerce, (b) trade and economic sanctions maintained by the U.S. Treasury Department’s Office of Foreign Assets Control, and (c) the International Traffic in Arms Regulations (“ITAR”) maintained by the U.S. Department of State.

“Fees” means the product of the amount of Services or Software used or ordered by Customer multiplied by the Prices, plus any applicable Taxes. Fees will be described in the Customer’s Reseller Agreement or Distributor Agreement.

“Google” means Google LLC and its Affiliates, including Google Public Sector LLC.

“Google Indemnified Materials” has the meaning described in the applicable Services Schedule.

“High Risk Activities” means activities where the use or failure of the Services would reasonably be expected to result in death, serious personal injury, or severe environmental or property damage (such as the creation or operation of weaponry).

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time, and any regulations issued under it.

“including” means including but not limited to.

“Indemnified Liabilities” means any (a) settlement amounts approved by the indemnifying party, and (b) damages and costs finally awarded against the indemnified party 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.

“Legal Process” means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, 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” has the meaning described in the applicable Services Schedule.

“Order Form” has the meaning described in the applicable Services Schedule.

“Order Term” means the period of time starting on the Services Start Date for the Services and continuing for the period indicated on the Order Form unless terminated in accordance with the Agreement.

“Prices” has the meaning described in the applicable Reseller Agreement or Distributor Agreement.

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

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

“Service Level Agreement” or “SLA” has the meaning described in the Services Schedule (if applicable).

“Services” has the meaning described in the applicable Services Schedule.

“Services Schedule(s)” means a schedule to the Agreement with terms that apply only to the services and software (if applicable) described in that schedule.

“Services Start Date” means either the start date described in the Order Form or, in the absence of any such date, the date Google makes the Services available to Customer.

“Software” has the meaning described in the Services Schedule (if applicable).

“Suspend” or “Suspension” means disabling or limiting access to or use of the Services or components of the Services.

“Taxes” 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 described at https://www.google.com/permissions/trademark/brand-terms.html.

“URL” means a uniform resource locator address to a site on the internet.

“URL Terms” has the meaning described in the Services Schedule (if applicable).

“Use Restrictions” means the restrictions in Section 2.3 (Use Restrictions) of these General Terms and any additional restrictions on the use of Services described in a section entitled “Additional Use Restrictions” in the applicable Services Schedule.

Google Cloud Master Agreement
Google Cloud Platform Services Schedule

This Google Cloud Platform Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement. This Services Schedule applies solely to the services and software described in this Services Schedule and is effective for the Term of the Agreement. Terms defined in the General Terms apply to this Services Schedule.

1. Using the Services.

1.1 Admin Console. Google (or Reseller or Distributor) will provide Customer an Account to access the Admin Console through which Customer may manage its use of the Services. Customer is responsible for (a) maintaining the confidentiality and security of the Account and associated passwords and (b) any use of the Account.

1.2 Ceasing Services Use. Customer may stop using the Services at any time.

1.3 Customer Applications. Customer may enable End Users to access its Customer Applications.

1.4 Additional Use Restrictions. Unless otherwise permitted in the GCP Service Specific Terms, Customer will not (a) use, and will not allow End Users to use, the Services to operate or enable any telecommunications service, or to place or receive calls from any public switched telephone network, including as part of a Customer Application; or (b) use the Services to provide a hosting, outsourced, or managed services solution to unaffiliated third parties, except as part of a Customer Application that provides value distinct from the Services.

2. Data Processing and Security.

2.1 Protection of Customer Data. Google will only access or use Customer Data to provide the Services and TSS ordered by Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards to protect Customer Data, as further described in the Data Processing Addendum.

2.2 Data Processing Addendum. The Data Processing Addendum is incorporated by reference into this Services Schedule.

3. Additional Payment Terms.

3.1 Usage and Invoicing. Customer will pay all Fees for the Services and GCP Technical Support Services. Google's measurement tools will be used to determine Customer's usage of the Services. Each invoice, which may be generated by Reseller or Distributor, will include data in sufficient detail to allow Customer to validate the Services purchased and associated Fees.

3.2 RESERVED.

3.3 RESERVED.

4. Updates to Services and Terms.

4.1 Changes to Services.

(a) Limitations on Changes. Google may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services.

(b) Discontinuance. Google will notify Customer at least 12 months before discontinuing any Service

(or associated material functionality), and at least 36 months for any Key Service (or associated material functionality), in each case unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

(c) Support. Google will continue to provide product and security updates, and GCP Technical Support Services, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).

(d) Backwards Incompatible Changes. Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner.

4.2 Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing Addendum, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms. No change shall be inconsistent with the provisions of 48 C.F.R. 552.212-4(w).

4.3 Permitted Changes. Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to new or pre-general availability Services, offerings, or functionality.

5. Temporary Suspension.

5.1 Services Suspension. Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Customer or any End User's use of the Services does not comply with the AUP, and it is not cured following notice from Google.

5.2 Limitations on Services Suspensions. If Google Suspends Services under Section 5.1 (Services Suspension), then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

6. Technical Support. Google will provide GCP Technical Support Services to Customer during the Order Term in accordance with the GCP Technical Support Services Guidelines. Customer is responsible for the technical support of its Customer Applications and Projects.

7. Copyright. Google provides information to help copyright holders manage their intellectual property online, but Google cannot determine whether something is being used legally without input from the copyright holders. Google will respond to notices of alleged copyright infringement and may terminate repeat infringers in appropriate circumstances as required to maintain safe harbor for online service providers under the U.S. Digital Millennium Copyright Act. If Customer believes a person or entity is infringing Customer's or its End User's copyrights and would like to notify Google, Customer can find information about submitting notices, and Google's policy about responding to notices, at http://www.google.com/dmca.html.

8. Software.

8.1 Provision of Software. Google may make Software available to Customer, including third-party software. Customer's use of any Software is subject to the applicable provisions in the GCP Service Specific Terms.

8.2 Ceasing Software Use. If the Agreement or the Google Cloud Platform Order Form terminates or expires, then Customer will stop using the Software.

9. Survival. The following Sections of this Services Schedule will survive expiration or termination of this Services Schedule: Section 11 (Additional Definitions).

10. **Termination of Previous Agreements.** If Google and Customer have previously entered into a Google Cloud Platform License Agreement, then that agreement will terminate on the Services Start Date, and the Agreement will govern the provision and use of the Services going forward.

11. **Additional Definitions.**

"Account" means Customer's Google Cloud Platform account.

"Admin Console" means the online console(s) or dashboard provided by Google to Customer for administering the Services.

"AUP" means the then-current acceptable use policy for the Services described at https://cloud.google.com/terms/aup.

"Covered Affiliate" means an Affiliate using the Services under Customer's Account.

"Customer Application" means a software program that Customer creates or hosts using the Services.

"Customer Data" means 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 Services.

"Customer Indemnified Materials" means Customer Data, Customer Brand Features, Customer Applications, and Projects.

"Data Processing Addendum" means the then-current terms describing data processing and security obligations with respect to Customer Data, as described at https://cloud.google.com/terms/data-processing-terms.

"End User" or "Customer End User" means an individual that Customer permits to use the Services or a Customer Application. For clarity, End Users may include employees of Customer Affiliates and other authorized third parties.

"GCP Service Specific Terms" means the then-current terms specific to one or more Services or Software described at https://cloud.google.com/cloud/terms/service-terms.

"GCP Technical Support Services" or "TSS" means the then-current technical support service provided by Google to Customer under the GCP Technical Support Services Guidelines.

"GCP Technical Support Services Guidelines" or "TSS Guidelines" means the then-current Google Cloud Platform support service guidelines described at https://cloud.google.com/terms/tssg/.

"Google API" means any application programming interface provided by Google as part of the Services.

"Google Indemnified Materials" means the Services and Google's Brand Features.

"Key Services" means the then-current list of Services described at https://cloud.google.com/terms/key-services. Google may not remove a Service from this URL unless that Service is discontinued in accordance with Section 4.1(b) (Discontinuance).

"Notification Email Address" means the email address(es) designated by Customer in the Admin Console.

"Order Form" means an order form issued by Google, Reseller or Distributor and executed by Customer and issuer specifying the Services Google will provide to Customer under this Services Schedule.

“Prices” means the applicable prices described in the applicable Reseller Agreement or Distributor Agreement.

“Project” means a collection of Google Cloud Platform resources configured by Customer via the Services.

“Services” means the then-current services described at https://cloud.google.com/terms/services, excluding any Third-Party Offerings.

“SLA” means the then-current service level agreements described at https://cloud.google.com/terms/sla/.

“Software” means any downloadable tools, software development kits, or other such computer software provided by Google for use in connection with the Services, and any updates Google may make to such Software from time to time, excluding any Third-Party Offerings.

“Third-Party Offerings” means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software and (b) offerings identified in the "Third-Party Terms" section of the Service Specific Terms.

“URL Terms” means the AUP, Data Processing Addendum, GCP Service Specific Terms, GCP Technical Support Services Guidelines, and SLAs.

Google Cloud Master Agreement
Google Workspace Services Schedule

This Google Workspace Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement. This Services Schedule applies solely to the services described in this Services Schedule and is effective for the Term of the Agreement. Terms defined in the General Terms apply to this Services Schedule.

1. Using the Services.

1.1 Admin Console. Google will provide Customer access to the Admin Console through which Customer may manage its use of the Services. Customer may specify one or more Administrators through the Admin Console who will have the right to access Admin Accounts. Customer is responsible for (a) maintaining the confidentiality and security of the End User Accounts and associated passwords and
(b) any use of the End User Accounts. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer.

1.2 Additional Use Restrictions. Unless otherwise permitted in the Google Workspace Service Specific Terms, Customer will not use, and will not allow End Users to use, the Services to place or receive emergency services calls.

1.3 Adding End User Accounts During Order Term. Customer may purchase additional End User Accounts during an Order Term by means of an additional Order Form or Reseller Order or by ordering via the Admin Console. Such additional End User Accounts will have a pro-rated term ending on the last day of the applicable Order Term.

2. Data Processing and Security.

2.1 Data Processing Addendum. The Data Processing Addendum is incorporated by reference into this Services Schedule.

3. Additional Payment Terms.

3.1 Usage and Invoicing. Customer will pay all Fees for the Services and such payment will be made pursuant to the Reseller Agreement or Distributor Agreement. Google's measurement tools will be used to determine Customer's usage of the Services. Unless otherwise provided in the Agreement or required by law, Fees for Services are nonrefundable.

3.2 RESERVED.

4. Updates to Services and Terms.

4.1 Changes to Services.

(a) Limitations on Changes. Google may update the Services, provided the updates do not result in a material reduction of the performance or security of the Services.

(b) Discontinuance. Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality), and at least 36 months for any Key Service (or associated material functionality), in each case unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

(c) Support. Google will continue to provide product and security updates, and Technical Support Services, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).

4.2 Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing Addendum, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms. No change shall be inconsistent with the provisions of 48 C.F.R. 552.212-4(w)

4.3 Permitted Changes. Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to new or pre-general availability Services, offerings, or functionality.

5. Temporary Suspension.

5.1 Services Suspension. Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Reserved. For Suspensions of End User Accounts, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

5.2 Limitations on Services Suspensions. If Google Suspends Services, then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

6. Technical Support. Google will provide Google Workspace Technical Support Services to Customer during the Order Term in accordance with the Google Workspace Technical Support Services Guidelines.

7. Additional Customer Responsibilities.

7.1 Customer Domain Name Ownership. Customer is responsible for obtaining and maintaining any rights necessary for Customer's and Google's use of the Customer Domain Names under the Agreement. Before providing the Services, Google may require that Customer verify that Customer owns or controls the Customer Domain Names. If Customer does not own or control the Customer Domain Names, then Google will have no obligation to provide the Services to Customer.

7.2 Abuse Monitoring. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names, but Google may monitor emails sent to these aliases to allow Google to identify Services abuse.

8. Using Brand Features Within the Services. Google will display only those Customer Brand Features that Customer authorizes Google to display by uploading them into the Services. Google will display those Customer Brand Features within designated areas of the web pages displaying the Services to End Users. Customer may specify the nature of this use in the Admin Console. Google may also display Google Brand Features on such web pages to indicate that the Services are provided by Google.

9. Additional Products. Google makes optional Additional Products available to Customer and its End Users. Customer's use of Additional Products is subject to the Additional Product Terms.

10. RESERVED.

11. Termination of Previous Agreements. If Google and Customer have previously entered into another agreement under which Customer uses 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.

12. Additional Definitions.

"Additional Products" means products, services, and applications that are not part of the Services but may be accessible for use in conjunction with the Services.

"Additional Product Terms" means the then-current terms at https://workspace.google.com/intl/en/terms/additional_services.html.

"Admin Account" means a type of End User Account that Customer (or Reseller, if applicable) may use to administer the Services.

"Admin Console" means the online console(s) or dashboard provided by Google to Customer for administering (a) the Services and (b) the services set out in a Complementary Product Services Summary (if applicable).

"Administrator" means Customer-designated personnel who administer the Services to End Users on Customer's behalf, and have the ability to access Customer End User Accounts. Such access includes the ability to access, monitor, use, modify, withhold, or disclose any data available to End Users associated with their End User Accounts.

"AUP" means the then-current acceptable use policy for the Services described at https://workspace.google.com/terms/use_policy.html.

"Complementary Product Services Summary" has the meaning given in the Data Processing Addendum.

"Core Services" means the then-current "Core Services" as described in the Services Summary at https://workspace.google.com/terms/user_features.html, excluding any Third-Party Offerings.

"Covered Affiliate" means an Affiliate using the Services under Customer's Account.

"Customer Data" means data submitted, stored, sent, or received via the Services by Customer or its End Users.

"Customer Domain Name" means a domain name specified in the Order Form or Reseller Order to be used in connection with the Services.

"Customer Indemnified Materials" means Customer Data and Customer Brand Features.

"Data Processing Addendum" means the then-current terms describing data protection and processing obligations with respect to Customer Data, as described at https://cloud.google.com/terms/data-processing-addendum/

"End User" or "Customer End User" means an individual that Customer permits to use the Services. For clarity, End Users may include employees of Customer Affiliates and other authorized third parties.

"End User Account" means a Google-hosted account established by Customer through the Services for an End User to use the Services.

"GDPR" has the meaning given to it in the Data Processing Addendum.

"Google Indemnified Materials" means the Services and Google's Brand Features.

"Google Workspace Service Specific Terms" means the then-current terms specific to one or more Services

described at https://workspace.google.com/terms/service-terms/.

“Google Workspace Technical Support Services” or “TSS” means the technical support service provided by Google to Customer under the Google Workspace Technical Support Services Guidelines.

“Google Workspace Technical Support Services Guidelines” or “TSS Guidelines” means the then-current Google Workspace support service guidelines described at https://workspace.google.com/terms/tssg.html.

“Key Services” means Gmail, Google Calendar, Google Docs, Google Sheets, Google Slides, Google Drive, Google Chat, Google Meet, and Google Forms.

“Notification Email Address” means the email address(es) designated by Customer in the Admin Console.

“Order Form” means an order form issued by Google, Reseller or Distributor and executed by Customer and issuer specifying the Services Google will provide to Customer under this Services Schedule.

“Other Services” means the then-current “Other Services” as described in the Services Summary at https://gsuite.google.com/terms/user_features.html, excluding any Third-Party Offerings.

“Personal Data” has the meaning given to it in the Data Processing Addendum.

“Prices” means the applicable prices described in the applicable Reseller Agreement or Distributor 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.

“Services” means the then-current Core Services and Other Services described at https://workspace.google.com/terms/user_features.html.

“SLA” means the then-current service level agreement described at https://gsuite.google.com/terms/sla.html.

“Third-Party Offerings” means third-party services, software, products, and other offerings that are not incorporated into the Services.

“URL Terms” means the AUP, Data Processing Addendum, Google Workspace Service Specific Terms, Google Workspace Technical Support Services Guidelines, and SLAs.

Google Cloud Master Agreement
Implementation Services Schedule

This Implementation Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement. This Services Schedule applies to implementation and advisory services described in this Services Schedule that are designed to help Customer use Google products and services. Terms defined in the General Terms apply to this Services Schedule.

1. Services.

1.1 Provision of Services. Google will provide Services, including Deliverables, to Customer, subject to Customer fulfilling its obligations under Section 2.1 (Cooperation).

1.2 Training Services. Customer may order Training Services for use in connection with the Services. Training Services are subject to the Training Terms.

1.3 Invoices and Payment. Customer will pay all Fees for Services ordered under this Services Schedule. Fees for some Services may be non-cancellable, as specified in the Order Form.

1.4 Personnel. Google will determine which Personnel will perform the 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.

1.5 Compliance with Customer's Onsite Policies and Procedures. Google Personnel performing Services at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.

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 the information, materials, consents, or access to Customer facilities, networks, or systems required for Google to perform the Services. If Reseller, Distributor or Google informs Customer of such failure and Customer does not cure the failure within 30 days, then (a) Reseller, Distributor or Google may seek to terminate any incomplete Services pursuant to FAR 52.233-1 as a termination for convenience under FAR 52.249-2.

2.2 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.

1.1 Customer will reimburse expenses (a) specifically described in the applicable Reseller Order Form; or (b) up to the amounts specified as "expenses" in the applicable Reseller Order Form that are actual, reasonable, and necessary.

2. Intellectual Property.

2.1 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 Services (with a right to sublicense to Google Affiliates and subcontractors). Except for the license rights under Sections 3.2 (Google Technology) and 3.3 (Deliverables), neither party will acquire any right, title, or interest in the other party's Background IP under this Services Schedule.

2.2 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 (with the right to sublicense to Affiliates) to use the Google Technology in connection with the Deliverables for Customer's internal business purposes. This Services Schedule does not grant Customer any right to use materials, products, or services that are made available to Google customers under a separate agreement, license, or Services Schedule.

2.3 Deliverables. Google grants Customer a limited, worldwide, non-exclusive, perpetual, fully-paid, non-transferable license (with the right to sublicense to Affiliates) to use, reproduce, and modify the Deliverables for Customer's internal business purposes.

3. Warranties and Remedies.

3.1 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 requisite skills, experience, and qualifications to perform the Services.

3.2 Remedies. Google's entire liability and Customer's sole remedy for Google's failure to provide Services that conform with Section 4.1 (Google Warranty) will be for Google to, at its option, (a) use commercially reasonable efforts to re-perform the Services or (b) terminate the Order Form and refund any applicable Fees received for the nonconforming Services. Any claim that Google has breached the warranty as described in Section 4.1 (Google Warranty) must be made within 30 days after Google has performed the Services.

4. Indemnification.

4.1 Indemnification Exclusions. General Terms Sections 9.1 (Google Indemnification Obligations) and 9.2 (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.

4.2 Infringement Remedies. The remedies described in General Terms Section 9.5 (Remedies) also apply to Deliverables.

5. Effects of Termination. If this Services Schedule or an Order Form under this Services Schedule expires or terminates, 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 6 (Effects of Termination), and Google will stop work on the Services.

(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) any remaining non-cancellable Fees. Google, Reseller, or Distributor will send Customer a final invoice for payment obligations under the Order Form.

(c) Survival. The following Sections of this Schedule will survive expiration or termination of this Services Schedule: 3 (Intellectual Property), 5 (Indemnification), 6 (Effects of Termination), and 9 (Additional Definitions).

6. **RESERVED**.

7. Termination of Previous Agreements. If Reseller, Distributor or Google and Customer have

previously entered into an agreement for Google to perform similar implementation services (including a Professional Services Agreement), then that agreement will terminate on the date of the last party's signature effectuating this Services Schedule, and the Agreement will govern the provision and use of the Services going forward.

8. 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.

"Covered Affiliate" means an Affiliate receiving the Services under this Services Schedule.

"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.

"Deliverables" means work product created for Customer by Google Personnel as part of the Services and specified as Deliverables in an Order Form.

"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.

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

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

"Personal Data" means personal data that: (a) has the meaning given to it in: (i) 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 ("EU GDPR"); or (ii) the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force ("UK GDPR"), as applicable; and (b) would cause Google to be subject to the EU GDPR or the UK GDPR (as applicable) as a data processor for Customer.

"Personnel" means a party's and its Affiliates' respective directors, officers, employees, agents, and subcontractors.

"Prices" means the applicable prices described in the applicable Reseller Agreement or Distributor Agreement.

"Services" means the then-current advisory and implementation services described at https://g.co/cloudpsoterms and an applicable Order Form and similar advisory or implementation services designed to help Customer use Google products and services. Services do not include Training Services.

"Training Services" means education and certification services related to Google products and services for individual users, as more fully described in an applicable Order Form. Training Services do not include

Deliverables.

“Training Terms” means the then-current terms applicable to Training Services described at https://enterprise.google.com/terms/training-services.html

Google Cloud Master Agreement - U.S. Public Sector Partner
Looker Services Schedule

This Looker Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement between the same parties to this Services Schedule. This Services Schedule applies solely to the services and software described in this Services Schedule and is effective for the Term of the Agreement. Terms defined in the General Terms apply to this Services Schedule.

1. **Using the Services.**

1.1. Use by Customer. Google (or Reseller or Distributor) will provide the Services to Customer by (a) providing access to an Instance for the Looker Hosted Deployment or (b) providing a license key for the Customer Hosted Deployment. Customer may only use the Services with databases and servers licensed and/or owned by Customer. Customer may configure the Services for Internal Business Purposes and External Business Purposes only to the extent authorized in the Order Form.

1.2. Use by Affiliates. Customer Affiliates may (i) access and use the Services as End Users, subject to the terms of Customer's Order Form so long as Customer remains responsible for the Affiliates' compliance with the Agreement and the applicable Order Form, or (ii) execute a separate Order Form that incorporates this Services Schedule by reference.

1.3. External Business Purposes. If the Order Form includes PBL and the PBL Client is bound to a written agreement with Customer that is at least as protective of Google as the rights and obligations contained in this Agreement, then Customer may make the Services available for use by PBL Users, including by embedding the Services into a Customer Application. Customer may not accept, and acknowledges that Google will not be bound by, any terms or conditions with the PBL Client that modify add to or change in any way the Agreement or Order Form.

1.4. Customer Responsibilities. Customer will be solely responsible, and Google disclaims responsibility for any acquisition, implementation, support or maintenance of third-party products or services purchased by Customer that may interoperate with the Services.

1.5. Additional Use Restrictions. Customer will not, and will not allow End Users to: (a) remove any copyright notices, trademarks or other proprietary notices or restrictions from the Services; (b) provide the Services on a time sharing, hosting, service provider or other similar basis, except as part of a Customer Application for External Business Purposes; (c) provide or obtain unauthorized access to the Services, including by sharing the log-on credentials for any End User with others; (d) circumvent any technical measures in the Software or Services; (e) conduct benchmarking tests or other comparative analysis of the Services for publication or disclosure to third parties or (f) disrupt the security, integrity or performance of the Services in any way.

1.6. Beta Features. Google may make Beta Features available to End Users subject to the provisions in the Looker Service Specific Terms.

2. **Data Processing and Security.** To the extent Customer provides Google with access to Customer Data under this Services Schedule, the following will apply:

2.1. Protection of Customer Data. Google will only access or use Customer Data to provide the Services and TSS ordered by Customer to Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards designed to protect the confidentiality, security, integrity, availability, and privacy of Customer Data stored in the Instance, as further described in the Data Processing Addendum. Notwithstanding any other provision of the Agreement, this Services Schedule or any other agreement related to the Services, Google will not be responsible for any breach or loss to the extent resulting from Customer's security configuration or Customer's administration of the Services.

2.2. Data Processing Addendums. The Data Processing Addendum is incorporated by reference into this Services Schedule.

3. Additional Payment Terms.

3.1. Usage and Invoicing. Customer will pay all Fees for the Services and TSS. Unless otherwise provided in the Agreement, the applicable Order Form or required by law, Fees for Services are non-refundable. Google's measurement tools will be used to determine Customer's usage of the Services. Each invoice, which shall be generated by Reseller or Distributor, will include data in sufficient detail to allow Customer to validate the Services purchased and associated Fees. If Customer exceeds the number of End Users, Scope of Use, or Deployment Attributes, Customer or the applicable Reseller or Distributor will, upon becoming aware, promptly notify the other party and the parties agree to discuss in good faith the additional Fees due by Customer for such over-deployment. The agreed upon additional Fees associated with the over-deployment will be memorialized in a new Order Form.

3.2. Additional Usage. Customer may purchase additional Deployment Attributes (including adding End Users) during an Order Term by executing an additional Order Form. Such purchase will have a pro-rated term ending on the last day of the applicable Order Term. Deployment Attributes cannot be decreased during the Order Term.

3.3. [RESERVED]

3.4. Services Use Review. Within 30 days of Google's reasonable written request, Customer will provide a sufficiently detailed written usage report listing the Deployment Attributes being used for each Scope of Use, the number and type of End Users using the Services during the requested period, and the Instance(s) deployed, along with the related license key(s). To the extent the usage reports can be measured by a ping from Google's license server, the ping will serve as the report. If there is a PBL deployment, Customer will provide a complete list of the software and applications where the Software and Services are deployed. If requested, Customer will provide reasonable assistance and access to information to verify the accuracy of any information provided to Google, which verification may include access to records relating to Customer's use of the Services. If the review indicates an underpayment, Customer agrees to negotiate in good faith a new or replacement Order Form that will cover the additional usage.

4. Updates to Services and Terms.

4.1. Changes to Services.

(a) Limitations on Changes. Google may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services.

(b) Discontinuance. Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality), unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

(c) Support. Google will continue to provide product and security updates, and TSS, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).

4.2. Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing Addendum(if applicable), or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms. No change shall be inconsistent with the provisions of 48 C.F.R. 552.212-4(w)

4.3. Permitted Changes. Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to Beta Features or new or pre-general availability Services, offerings, or functionality.

5. **Temporary Suspension.**

5.1. Services Suspension. Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Reserved. For Suspensions of End User Accounts, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

5.2. Limitations on Services Suspensions. If Google Suspends Services under Section 5.1 (Services Suspension), then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

6. **Technical Support.** Unless otherwise agreed in an Order Form, Google will provide Looker Technical Support Services to Customer during the Order Term in accordance with the Looker Technical Support Services Guidelines. Customer is responsible for the technical support of its Customer Applications, including PBL Users using the Services for External Business Purposes.

7. **Provision of Software.** Google may make Software available to Customer in connection with Customer's use of the Services, including third-party software. Some Software may be subject to third-party license terms, which can be found at: https://looker.com/terms/notices-and-acknowledgements.

8. **Ceasing Software Use.** If the Agreement, this Services Schedule or the Order Form for the Services terminates or expires, then Customer will stop using the Software.

9. [RESERVED]

10. **Professional Services**. If Customer purchases PSO Services, such PSO Services will be provided in accordance with a separate agreement and not under this Services Schedule.

11. **Survival.** The following section of this Services Schedule will survive expiration or termination of this Services Schedule: 3 (Additional Payment Terms) and Section 13 (Additional Definitions).

12. **Termination of Previous Agreements.** If Customer has previously entered into an agreement for the Software or Services, then that agreement will terminate on the Services Start Date, and this Agreement, including the Order Form referencing this Services Schedule, will govern the provision and use of the Services going forward.

13. **Additional Definitions.**

"AUP" means the then-current acceptable use policy for the Services described at https://cloud.google.com/terms/aup

"Beta Features" has the meaning set forth in the Looker Service Specific Terms.

"Covered Affiliate" means Customer's Affiliate using the Services (i) via an Order Form that is subject to the terms of this Services Schedule, and (ii) in compliance with the Agreement and the applicable Order Form.

"Customer Application" means a software program that Customer creates or hosts and that uses the Services. A Customer Application may be a website.

"Customer Data" means (a) all data in Customer's databases provided to Google by Customer or End Users via the Services and (b) all results provided to Customer or End Users for queries executed against such data via the Services.

“Customer Hosted Deployment” means the Software installed by or for Customer at Customer’s premises or on a Customer-controlled server within a data center selected and managed by Customer. A Customer Hosted Deployment includes the In-Product Services.

“Customer Indemnified Materials” means Customer Data and Customer Brand Features.

“Data Processing Addendum” or “DPA” means the then-current terms describing data processing and security obligations with respect to Customer Data described at https://looker.com/trust-center/legal/customers/dpst.

"Deployment Attributes" means the quantified usage of the Services as specified on an Order Form, which include, but are not limited to the number of Instances, End Users, API calls or other licensing attributes defined by the Scope of Use.

“Documentation” means the user guides and manuals for the Services provided by Google for all Customer’s own internal use.

"End User" or "Customer End User" means an individual that Customer permits to use the Services. End Users may include employees of Customer's Affiliates or PBL Users.

“External Business Purposes", “PBL” or “Powered by Looker” means use of the Services by or for the benefit of Customer’s customers or clients, and their users or other third parties.

“Google Indemnified Materials” means the Services, Software and Google’s Brand Features.

“In-Product Services” means the services hosted and made accessible by Google through the Software, specifically licensing data, configuration backups, system error reports, data actions and support tickets.

“Instance” means one single configuration of the Software's administrative settings and application database, subject to the platform restrictions detailed in the Order Form. Each Instance requires a unique license key to operate. Multiple identically configured Instances running with separate configurations are considered separate instances.

“Internal Business Purposes” means use of the Services by or for the benefit of Customer’s internal operations.

“Looker Hosted Deployment” means the Software installed by Google on a web connected platform that is run in a hosting facility designated by Google, unless otherwise agreed by the parties in an Order Form. A Looker Hosted Deployment includes the In-Product Services.

"Looker Service Specific Terms" means the then-current terms specific to the Services stated at https://looker.com/trust-center/legal/customers/service-terms

“Looker Technical Support Services” or “TSS” means the then-current technical support service provided by Google to Customer under the Looker Technical Support Services Guidelines.

“Looker Technical Support Services Guidelines” or “TSS Guidelines” means the then-current technical support service provided by Google to Customer described at https://looker.com/trust-center/legal/customers/support-lss.

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

“Order Form” means an order form issued by Google, Reseller or Distributor and executed by Customer and issuer specifying the Services Google will provide under this Services Schedule.

“PBL Client” means (i) the PBL User or (ii) Customer’s client that authorizes use of the Services by PBL Users.

“PBL User” is an individual authorized to use the Services for External Business Purposes as an End User subject to the terms of the applicable Order Form.

“Prices” means the prices agreed to by Customer and Reseller or Distributor in the applicable Reseller Agreement or Distributor Agreement.

“PSO Services” means advisory and consulting services purchased by Customer from Reseller or Distributor.

“Scope of Use” means Customer’s specific use case for the Services as defined in an Order Form, which may include limitations on Customer’s use for Internal Business Purposes and/or External Business Purposes.

“Services” means 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. Services exclude Third Party Offerings.

“SLA” means the then-current service level agreements applicable to the Looker Hosted Deployment only, described at https://looker.com/trust-center/legal/sla-lss.

“Software” means any downloadable tools, including the licensed data platform provided under the Services Schedule, and any other computer software provided by Google for use in connection with the Services, and any copies, modifications, derivative works or enhancements thereto, excluding any Third-Party Offerings.

“Third-Party Offerings” means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software and (b) offerings identified in the “Third-Party Offerings” section of the Looker Service Specific Terms.

“URL Terms” means the AUP, Data Processing Addendum, Looker Technical Support Services Guidelines, and the SLAs.

Google Cloud Platform Services Summary

The complete list of services that form Google Cloud Platform is shown below. While Google offers many other services and APIs, only the services below are covered by the Google Cloud Platform terms of service, service level agreements (if applicable), and support offerings. Offerings identified below as Software or Premium Software are not Services under the Google Cloud Platform Terms of Service and the Cloud Data Processing Addendum.

> Services marked in *asterisks* are not available for resale under the Google Cloud Partner Advantage program, unless specifically authorized in writing by Google.

Compute

App Engine: App Engine enables you to build and host applications on the same systems that power Google applications. App Engine offers fast development and deployment; simple administration, with no need to worry about hardware, patches or backups; and effortless scalability.

Batch: Batch is a fully-managed service that allows you to create batch jobs at scale. The service dynamically provisions certain Google Cloud resources, schedules your batch job on the resources, manages the queue for the job, and executes the job. Batch is natively integrated with Google Cloud services for storage, logging, monitoring, and more.

Compute Engine: Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud, with options to utilize certain CPUs, GPUs, or Cloud TPUs. You can use Compute Engine to solve large-scale processing and analytic problems on Google's computing, storage, and networking infrastructure.

Google Cloud VMware Engine (GCVE): GCVE is a managed VMware-as-a-Service that is specifically designed for running VMware workloads on Google Cloud Platform. GCVE enables customers to run VMware virtual machines natively in a dedicated, private, software-defined data center.

Storage

Cloud Storage: Cloud Storage is a RESTful service for storing and accessing your data on Google's infrastructure. The service combines the performance and scalability of Google's cloud with advanced security and sharing capabilities.

Persistent Disk: Persistent Disk is a durable and high performance block storage service for Google Cloud Platform. Persistent Disk provides SSD and HDD storage that can be attached to instances running in either Compute Engine or Google Kubernetes Engine.

Cloud Filestore: Cloud Filestore is a scalable and highly available shared file service fully-managed by Google. Cloud Filestore provides persistent storage ideal for shared workloads. It is best suited for enterprise applications requiring persistent, durable, shared storage which is accessed by NFS or requires a POSIX compliant file system.

***Cloud Storage for Firebase**: Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for your Firebase apps, as well as robust uploads and downloads regardless of network quality through the Firebase SDK. Cloud Storage for Firebase is backed by Cloud Storage, a service for storing and accessing your data on Google's infrastructure.

Databases

AlloyDB: AlloyDB is a fully-managed, PostgreSQL-compatible database for demanding transactional and analytical workloads. It is designed to provide enterprise-grade performance and availability while maintaining compatibility with open-source PostgreSQL.

Cloud Bigtable: Cloud Bigtable is a fast, fully-managed, highly-scalable NoSQL database service. It is designed for the collection and retention of data from 1TB to hundreds of PB.

Datastore: Datastore is a fully-managed, schemaless, non-relational datastore. It provides a rich set of query capabilities, supports atomic transactions, and automatically scales up and down in response to load. It can scale to support an application with 1,000 users or 10 million users with no code changes.

Firestore: Firestore is a NoSQL document database for storing, syncing, and querying data for mobile and web apps. Its client libraries provide live synchronization and offline support, while its security features and integrations with Firebase and Google Cloud Platform accelerate building serverless apps.

Memorystore: Memorystore, which includes Memorystore for Redis and Memorystore for Memcached, provides a fully-managed in-memory data store service that allows customers to deploy distributed caches that provide sub-millisecond data access.

Cloud Spanner: Cloud Spanner is a fully-managed, mission-critical relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and strong consistency at global scale.

Cloud SQL: Cloud SQL is a web service that allows you to create, configure, and use relational databases that live in Google's cloud. It is a fully-managed service that maintains, manages, and administers your databases, allowing you to focus on your applications and services.

Networking

Cloud CDN: Cloud CDN uses Google's globally distributed edge points of presence to cache HTTP(S) load balanced content close to your users.

Cloud DNS: Cloud DNS is a high performance, resilient, global, fully-managed DNS service that provides a RESTful API to publish and manage DNS records for your applications and services.

Cloud IDS (Cloud Intrusion Detection System): Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.

Cloud Interconnect: Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform using Google Services for Dedicated Interconnect, Partner Interconnect and Cloud VPN. This solution allows you to directly connect your on-premises network to your Virtual Private Cloud.

Cloud Load Balancing: Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications.

Cloud NAT (Network Address Translation): Cloud NAT enables instances in a private network to communicate with the internet.

Cloud Router: Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between your VPC network and your non-Google network.

Cloud VPN: Cloud VPN allows you to connect to your Virtual Private Cloud (VPC) network from your existing network, such as your on-premises network, another VPC network, or another cloud provider's network, through an IPsec connection using (i) Classic VPN, which supports dynamic (BGP) routing or static routing (route-based or policy-based), or (ii) HA (high-availability) VPN, which supports dynamic routing with a simplified redundancy setup, separate failure domains for the gateway interfaces, and a higher service level objective.

Google Cloud Armor: Google Cloud Armor offers a policy framework and rules language for customizing access to internet-facing applications and deploying defenses against denial of service attacks as well as targeted application attacks. Components of Google Cloud Armor include: L3/L4 volumetric DDos Protection, preconfigured web-application firewall (WAF) rules, and custom rules language.

Google Cloud Armor Managed Protection Plus: Google Cloud Armor Managed Protection Plus is a managed application protection service subscription that bundles Google Cloud Armor WAF and DDoS Protection with additional services and capabilities including DDoS response support, DDoS bill protection, and Google Cloud Armor Adaptive Protection, which is Google’s machine-learning based solution to protect internet-facing endpoints from network and application-based attacks.

Media CDN: Media CDN is a content delivery network that leverages Google’s global edge cache nodes to deliver exceptional caching efficiency and end user experiences.

Network Connectivity Center: Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.

Network Intelligence Center: Network Intelligence Center is Google Cloud’s comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-prem environments.

Network Service Tiers: Network Service Tiers enable you to select different quality networks (tiers) for outbound traffic to the internet: the Standard Tier primarily utilizes third party transit providers while the Premium Tier leverages Google's private backbone and peering surface for egress.

Service Directory: Service Directory is a managed service that offers customers a single place to publish, discover and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud, and on-prem environments and can scale up to thousands of services and endpoints for a single project.

Spectrum Access System: Spectrum Access System enables you to access the Citizens Broadband Radio Service (CBRS) in the United States, the 3.5 GHz band that is available for shared commercial use. You can use Spectrum Access System to register your CBRS devices, manage your CBRS deployments, and access a non-production test environment (if offered).

Traffic Director: Traffic Director is Google Cloud Platform's traffic management service for open service meshes.

Virtual Private Cloud: Virtual Private Cloud provides a private network topology with IP allocation, routing, and network firewall policies to create a secure environment for your deployments.

Operations

Cloud Debugger: Cloud Debugger connects your application's production data to your source code by inspecting the state of your application at any code location in production without stopping or slowing down your requests.

Cloud Logging: Cloud Logging is a fully-managed service that performs at scale and can ingest application and system log data, as well as custom log data from thousands of VMs and containers. Cloud Logging allows you to analyze and export selected logs to long-term storage in real time. Cloud Logging includes the Error Reporting feature, which analyzes and aggregates the errors in your cloud applications and notifies you when new errors are detected.

Cloud Monitoring: Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain Services, hosted uptime probes, application instrumentation, alert management, notifications and a variety of common application components.

Cloud Profiler: Cloud Profiler provides continuous profiling of resource consumption in your production applications, helping you identify and eliminate potential performance issues.

Cloud Trace: Cloud Trace provides latency sampling and reporting for App Engine, including per-URL statistics and latency distributions.

Developer Tools

Artifact Registry: Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols. This makes it simple to integrate it with your CI/CD tooling to set up automated pipelines.

Container Registry: Container Registry is a private Docker image storage system on Google Cloud Platform. The registry can be accessed through an HTTPS endpoint, so you can pull images from your machine, whether it's a Compute Engine instance or your own hardware.

Cloud Build: Cloud Build is a service that executes your builds on Google Cloud Platform infrastructure. Cloud Build can import source code from Cloud Storage, Cloud Source Repositories, GitHub, or Bitbucket; execute a build to your specifications; and produce artifacts such as Docker containers or Java archives.

Cloud Source Repositories: Cloud Source Repositories provides Git version control to support collaborative development of any application or service, including those that run on App Engine and Compute Engine.

***Firebase Test Lab**: Firebase Test Lab lets you test your mobile app using your test code or automatically on a wide variety of devices and device configurations hosted in a Google data center, with test results made available in the Firebase console.

Google Cloud Deploy: Google Cloud Deploy is a service for managing and performing application continuous delivery to Google Kubernetes Engine. It allows for process specification and control of application delivery.

Test Lab: Test Lab enables you to test mobile applications using physical and virtual devices in the cloud. It runs instrumentation tests and script-less robotic tests on a matrix of device configurations, and reports detailed results to help improve the quality of your mobile app.

Data Analytics

BigQuery: BigQuery is a fully-managed data analysis service that enables businesses to analyze Big Data. It features highly scalable data storage that accommodates up to hundreds of terabytes, the ability to perform ad hoc queries on multi-terabyte datasets, and the ability to share data insights via the web.

Cloud Composer: Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span across clouds and on-premises data centers. Cloud Composer allows you to use Apache Airflow without the hassle of creating and managing complex Airflow infrastructure.

Cloud Data Fusion: Cloud Data Fusion is a fully-managed, cloud native, enterprise data integration service for quickly building and managing data pipelines. Cloud Data Fusion provides a graphical interface to help increase time efficiency and reduce complexity and allows business users, developers, and data scientists to easily and reliably build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data without having to wrestle with infrastructure.

Cloud Life Sciences (formerly Google Genomics): Cloud Life Sciences provides services and tools for managing, processing, and transforming life sciences data.

Data Catalog: Data Catalog is a fully-managed and scalable metadata management service that empowers organizations to quickly discover, manage, and understand their data in Google Cloud. It offers a central data catalog across certain Google Cloud Services that allows organizations to have a unified view of their data assets.

Dataplex: Dataplex is an intelligent data fabric that helps customers unify distributed data and automate management and governance across that data to power analytics at scale.

Dataflow: Dataflow is a fully-managed service for strongly consistent, parallel data-processing pipelines. It provides an SDK for Java with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the life cycle of Compute Engine resources of the processing pipeline(s). It also provides a monitoring user interface for understanding pipeline health.

Datalab: Datalab is an interactive tool for exploration, transformation, analysis and visualization of your data on Google Cloud Platform. It runs in your cloud project and enables you to write code to use other Big Data and storage services using a rich set of Google-authored and third party libraries.

Dataproc: Dataproc is a fast, easy to use, managed Spark and Hadoop service for distributed data processing. It provides management, integration, and development tools for unlocking the power of rich open source data processing tools. With Dataproc, you can create Spark/Hadoop clusters sized for your workloads precisely when you need them.

Dataproc Metastore: Dataproc Metastore provides a fully-managed metastore service that simplifies technical metadata management and is based on a fully-featured Apache Hive metastore. Dataproc Metastore can be used as a metadata storage service component for data lakes built on open source processing frameworks like Apache Hadoop, Apache Spark, Apache Hive, Presto, and others.

Datastream: Datastream is a serverless change data capture (CDC) and replication service that enables data synchronization across heterogeneous databases, storage systems, and applications with minimal latency.

Google Earth Engine: Google Earth Engine is a platform for global-scale analysis and visualization of geospatial datasets. Google Earth Engine can be used with custom datasets, or with any of the publicly available satellite imagery hosted (and ingested on a regular basis) by Earth Engine Data Catalog.

***Looker Studio**: Looker Studio is a data visualization and business intelligence product. It enables customers to connect to their data stored in other systems, create reports and dashboards using that data, and share them throughout their organization.

- **Looker Studio Pro:** Looker Studio Pro is a paid edition of Looker Studio that adds enterprise governance, team management features, and other features listed at https://cloud.google.com/looker-studio/ or a successor URL. Unlike Looker Studio, Looker Studio Pro is eligible for partner resale.

Pub/Sub: Pub/Sub is designed to provide reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a "topic" and other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Pub/Sub allows developers to communicate between independently written applications.

AI and Machine Learning

AI Building Blocks

AutoML: AutoML is a machine learning product suite that enables developers with limited machine learning expertise to provide their data sets and obtain access to quality trained models produced by Google's transfer learning and Neural Architecture Search (Google's technology for finding, generating, evaluating, and training numerous neural architectures to automatically select a solution for the customer's application):

- **AutoML Natural Language**: AutoML Natural Language enables customers to categorize input text into their own custom defined labels (supervised classification). Users can customize models to their own domain or use case.
- **AutoML Tables**: AutoML Tables enables your entire team of data scientists, analysts, and developers to automatically build and deploy state-of-the-art machine learning models on structured data at increased speed and scale.
- **AutoML Translation**: AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited machine learning expertise to customize the Google Neural Machine Translation (GNMT) model for their own domain or use-case.
- **AutoML Video**: AutoML Video is a simple and flexible machine learning service that lets businesses and developers easily train custom and scalable video models for their own domain or use cases.
- **AutoML Vision**: AutoML Vision is a simple and flexible machine learning service that lets businesses and developers with limited machine learning expertise train custom and scalable vision models for their own use cases.

Cloud Natural Language API: Cloud Natural Language API provides powerful natural language understanding as an easy to use API. This API enables application developers to answer the following questions: 1) What are the entities referred to in the block of text?; 2) What is the sentiment (positive or negative) for this block of text?; 3) What is the language of this block of text?; and 4) What is the syntax for this block of text (including parts of speech and dependency trees)? Users can call this API by passing in a block of text or by referring to a document in Cloud Storage.

Cloud Translation (including Cloud Translation v2 or any subsequent general availability version/release): Cloud Translation is a RESTful API that automatically translates text from one language to another language (e.g. French to English). You can use the API to programmatically translate text in your webpages or apps.

Cloud Vision: Cloud Vision enables developers to understand the content of an image by encapsulating powerful machine learning models in an easy to use API. It quickly classifies images into thousands of categories (e.g., "sailboat", "lion", "Eiffel Tower"), detects individual objects and faces within images, and finds and reads printed words contained within images. You can build metadata on your image catalog, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. You can also analyze images uploaded in the request and integrate with your image storage on Cloud Storage.

Contact Center AI (CCAI): CCAI is a solution for improving the customer experience in your contact centers using AI. CCAI encompasses Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Speech-to-Text, and Text-to-Speech, and Speaker ID.

Contact Center AI Insights: Contact Center AI Insights helps customers extract value from their contact center data. It provides a console to explore the data, find relevant information and take action on the data. Customers can run advanced analysis within the platform to extract sentiment, topics and highlight key areas from their data.

Contact Center AI ("CCAI") Platform: CCAI Platform is an AI-driven contact-center-as-a-service (CCaaS) platform built natively on Google Cloud, leveraging Contact Center AI at its core. CCAI Platform is purpose-built to work alongside CRMs, providing organizations with a single source of truth for customer journeys. As a unified contact center platform, CCAI Platform accelerates the organization's ability to leverage and deploy AI-driven contact center functionalities without relying on multiple technology providers. CCAI Platform is a full-stack contact center platform for queuing and routing customer interactions across voice and digital channels. It provides easy routing of customer interactions to the appropriate resource pools, allowing a seamless transition to human agents.

Dialogflow Essentials(ES): Dialogflow is a development suite for voice and text conversational apps including chatbots and voicebots. Dialogflow is cross-platform and can connect to your own apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Telephony platforms like Genesys, Avaya, Cisco and digital platforms like Actions on Google, Facebook Messenger, Slack). Dialogflow Essentials Edition is a paid enterprise tier of Dialogflow provided under the Google Cloud Platform Terms of Service. (The free tier of Dialogflow (Dialogflow Trial Edition) is not offered via the Google Cloud Platform Terms of Service and is instead provided under the Dialogflow Trial Edition Terms of Service).

Dialogflow Customer Experience Edition (CX): Dialogflow CX is an advanced development suite for creating conversational AI applications including chatbots and voicebots. It includes a visual bot building platform, collaboration and versioning tools, bot modularization tools, advanced IVR feature support (like DTMF, barge-in, etc.), and is optimized for enterprise scale and complexity. Dialogflow CX is cross-platform and can connect to your own apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., telephony platforms like Genesys, Avaya, Cisco and digital platforms). Dialogflow CX is provided under the Google Cloud Platform Terms of Service.

Document AI: Document AI classifies and extracts structured data from documents to help discover insights and automate business processes.

- ***Human-in-the-Loop AI**: Human-in-the-Loop AI provides a user interface and workflow tools for human verification of data extracted from documents using Document AI.

Document AI Warehouse: Document AI Warehouse is a data management and governance platform that stores, searches, and organizes documents and their extracted and tagged metadata. Document AI Warehouse is highly scalable and fully managed, requiring no customer-deployed infrastructure, and can be integrated with enterprise document workflows, applications, and repositories.

Media Translation API: Media Translation API is a gRPC API that automatically translates audio from one language to another language (e.g., French to English) and supports streaming real time. You can use the API to programmatically translate audio in your apps.

***Speaker ID**: Speaker ID allows customers to enroll user voice prints and later verify users against a previously enrolled voice print.

Speech On Device: Speech On Device allows customers to deploy speech-to-text (STT) and text-to-speech (TTS) services locally on their custom embedded hardware and operating systems.

Speech-to-Text: Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy to use API.

Text-to-Speech: Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.

Timeseries Insights API: Timeseries Insights API is a service that enables large-scale time series forecasting and anomaly detection in real time. The API is designed to scale to billions of time series and their properties, and within a few seconds of implementation, detect trends, seasonality, and anomalies across the time series.

Vertex AI Vision: Vertex AI Vision is a service that allows you to easily build, deploy, and manage computer vision applications with a fully managed, end-to-end application development environment.

Video Intelligence API: Video Intelligence API makes videos searchable, and discoverable, by extracting metadata with an easy to use REST API. It quickly annotates videos stored in Cloud Storage, and helps you identify key noun entities of your video and when they occur within the video.

Visual Inspection AI: Visual Inspection AI enables developers to train and deploy AI models to automatically detect, classify, and localize abnormalities found in images in order to improve production quality and develop enhanced analytics across multiple industries.

Vertex AI, AI Platform, and Accelerators

AI Platform Data Labeling: AI Platform Data Labeling is a service that helps developers obtain high quality data to train and evaluate their machine learning models. It supports labeling for image, video, text, and audio as well as management of all of your labeled data in one place.

AI Platform Deep Learning Container: AI Platform Deep Learning Container is a Docker image with the most popular AI frameworks. Machine learning developers and data scientists can customize AI Platform Deep Learning Container and use it with AI Workbench (also known as Notebooks), Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

AI Platform Neural Architecture Search (NAS): NAS is a managed service leveraging Google's neural architecture search technology to generate, evaluate, and train numerous model architectures for a customer's application. NAS training services facilitate management of large-scale experiments.

AI Platform Training and Prediction: AI Platform Training and Prediction is a managed service that enables you to easily build and use machine learning models. It provides scalable training and prediction services that work on large scale datasets.

Vertex AI: Vertex AI is a service for managing the entire lifecycle of AI and machine learning development. With Vertex AI, you can (i) manage image, video, text, and tabular datasets and associated labels; (ii) build machine learning pipelines to train and evaluate models using Google Cloud algorithms or custom training code; (iii) deploy models for online or batch use cases all on scalable managed infrastructure (including additional discovery points and API endpoints for functionality replacing the legacy services of AI Platform Data Labeling, AI Platform Training and Prediction, AI Platform Neutral Architecture Search (NAS), AutoML Natural Language, AutoML Video, AutoML Vision, and AutoML Tables); (iv) manage your entire data science workflow using Vertex AI Workbench (also known as Notebooks), which offers Google and user-managed options for a notebook-based development environment, including JupyterLab instances; and (v) create realistic plans to optimize your business with Optimization AI and related functionality.

Industry Solutions

***Talent Solution**: Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Discovery Solutions: Discovery Solutions allow customers in retail, media, and other verticals to deliver Google-quality search results and recommendations on their own websites and mobile applications.

- ***Recommendations AI:** Recommendations AI enables you to build an end-to-end personalized recommendation system based on state-of-the-art deep learning ML models, without a need for expertise in ML or recommendation system architecture.
- ***Recommendationengine API:** Recommendationengine API is the Version 1 API of Recommendations AI described above. This API will be deprecated in 2023 and is not accepting new customers.
- ***Retail Search**: Retail Search, powered by Google's Retail API, allows retailers to leverage Google's search capabilities on their own retail websites and mobile applications. With Retail Search, retailers receive fast, accurate, and high quality search results that help improve conversion and increase customer engagement.

API Management

Apigee and Apigee Edge: Apigee and Apigee Edge are full-lifecycle API management platforms that let customers design, secure, analyze, and scale APIs, giving them visibility and control.

- **Apigee:** Apigee is available as Apigee X, a fully-managed service, and as Apigee hybrid, a hybrid model that's partially hosted and managed by the customer.
- **Apigee Edge:** Apigee Edge is available as a fully-managed service and as Apigee Private Cloud, a customer-hosted Premium Software solution.

API Gateway: API Gateway is a fully-managed service that helps you develop, deploy, and secure your APIs running on Google Cloud Platform.

Cloud Endpoints: Cloud Endpoints is a tool that helps you to develop, deploy, secure and monitor your APIs running on Google Cloud Platform.

Payment Gateway: Payment Gateway is a managed service that provides a reliable, scalable and secure way for customers to integrate with real time payment systems like Unified Payments Interface (UPI).

- **Issuer Switch:** Issuer Switch provides customers with a managed deployment of standard payment interfaces for performing payment and non-payment transactions on their users' accounts.

Hybrid and Multi-cloud

Anthos: Anthos is a solution designed for building and managing modern applications running across hybrid cloud environments. Anthos is an integrated platform incorporating cloud-based services and software components, including:

- **Anthos Config Management**: Anthos Config Management is a policy management solution for enabling consistent configuration across multiple Kubernetes clusters. Anthos Config Management allows you to specify one single source of truth and then enforce those policies on your cluster.
- **Anthos Identity Service**: Anthos Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple Anthos environments. Users can log in to and access their Anthos clusters from the command line or from the Google Cloud console, all using their existing identity providers.
- **Anthos Integration with Google Cloud Platform Services**: Google Cloud Platform services and components may be used in connection with Anthos deployments, including Google Kubernetes Engine (GKE), Cloud Logging, Cloud Monitoring, Traffic Director, and Google Cloud Platform Marketplace.
- **Anthos Premium Software**: Anthos includes the software components listed below as Premium Software.
- **Anthos Service Mesh**: Anthos Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Anthos Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. For clarity this service does not include Anthos Service Mesh -- Software (see below regarding Premium Software).

- **Google Kubernetes Engine**: Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, enables you to run containers on Google Cloud Platform. Kubernetes Engine takes care of provisioning and maintaining the underlying virtual machine cluster, scaling your application, and operational logistics such as logging, monitoring, and cluster health management.
- **Connect**: Connect is a service that enables both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.
- **Hub**: Hub is centralized control-plane that enables a user to register clusters running in a variety of environments, including Google's cloud, on premises in customer datacenters, or other third party clouds. Hub provides a way for customers to centrally manage features and services on customer-registered clusters.

Cloud Run for Anthos: Cloud Run for Anthos lets you run stateless containers on Anthos.

Google-Managed Multi-Cloud Services

***BigQuery Omni:** BigQuery Omni is a Google-managed multi-cloud analytics solution that enables analysts to access and analyze data stored on other supported public clouds from a singular BigQuery control-plane on GCP.

Bare Metal

Bare Metal Solution: Bare Metal Solution allows you to operate and manage dedicated bare metal hardware (servers and attached storage) in Google's subprocessors' data centers to run specialized workloads with low latency.

Migration

BigQuery Data Transfer Service: BigQuery Data Transfer Service automates data movement from SaaS applications to BigQuery on a scheduled, managed basis. With the BigQuery Data Transfer Service, you can transfer data to BigQuery from SaaS applications including Google Ads, Campaign Manager, Google Ad Manager, and YouTube.

BigQuery Migration Service: BigQuery Migration Service is a solution for migrating your existing data warehouse to BigQuery. It includes tools, such as batch and interactive SQL translators, that can help with each phase of migration from assessment and planning to execution and verification.

Database Migration Service: Database Migration Service is a fully-managed migration service that makes it simple to perform high fidelity, minimal-downtime migrations at scale. You can use Database Migration Service to migrate from your on-premises environments, Compute Engine, and other clouds to certain Google Cloud-managed databases with minimal downtime.

Google Distributed Cloud Edge Appliance Service: Google Distributed Cloud Edge Appliance Service allows you to run private Google Kubernetes Engine clusters on ruggedized hardware deployed on customer premises. You can use Google Distributed Cloud Edge Appliance Service to offload sensor data for storage, low latency processing, and ML/AI inference in bandwidth-limited locations.

Migration Center: Migration Center enables you to automatically discover your existing infrastructure, analyze the cost benefits of public cloud, and facilitate planning your migration to Google Cloud.

Migrate to Virtual Machines: Migrate to Virtual Machines is a fully-managed migration service that enables you to migrate workloads at scale into Google Cloud Compute Engine with minimal down time by utilizing replication-based migration technology.

Storage Transfer Service: Storage Transfer Service enables you to import large amounts of online data into Cloud Storage, quickly and cost-effectively. With Storage Transfer Service, you can transfer data from locations reachable by the general internet (e.g., HTTP/HTTPS), including Amazon Simple Storage Service (Amazon S3), as well as transfer data between Google Cloud products (e.g., between two Cloud Storage buckets). You can also use Storage Transfer Service to move data between private data center storage (e.g., NFS) and Google Cloud products (e.g., transfer from NFS to Cloud Storage).

Transfer Appliance: Transfer Appliance is a solution that uses hardware appliances and software to transfer large amounts of data quickly and cost-effectively into Google Cloud Platform.

Security and Identity

Security

Access Transparency: Access Transparency captures near real-time logs of manual, targeted accesses by Google administrators, and serves them to customers via their Cloud Logging account.

Assured Workloads: Assured Workloads provides functionality to create security controls that are enforced on your cloud environment. These security controls can assist with your compliance requirements (for example, FedRAMP Moderate).

Binary Authorization: Binary Authorization helps customers ensure that only signed and explicitly-authorized workload artifacts are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

Certificate Authority Service: Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Certificate Authority Service can be used to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.

Certificate Manager: Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.

Cloud Asset Inventory: Cloud Asset Inventory is an inventory of cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

Cloud Data Loss Prevention: Cloud Data Loss Prevention is a fully-managed service designed to help you discover, classify, and protect your most sensitive data. You can inspect, mask, and de-identify sensitive data like personally identifiable information (PII).

Cloud External Key Manager (Cloud EKM): Cloud EKM lets you encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.

Cloud HSM: Cloud HSM (Hardware Security Module) is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys.

Cloud Key Management Service: Cloud Key Management Service is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on premises. You can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys.

Event Threat Detection: Event Threat Detection helps detect threats in log data. Threat findings are written to Security Command Center and optionally to Cloud Logging.

Key Access Justifications (KAJ): KAJ provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.

Risk Manager: Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

Security Command Center: Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center provides asset inventory and discovery and allows you to identify misconfigurations, vulnerabilities and threats, helping you to mitigate and remediate risks.

VPC Service Controls: VPC Service Controls provide administrators the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks, thereby mitigating data exfiltration risks.

Secret Manager: Secret Manager provides a secure and convenient method for storing API keys, passwords, certificates, and other sensitive data.

Web Security Scanner: Web Security Scanner is a web application security scanner that enables developers to easily check for a subset of common web application vulnerabilities in websites built on App Engine and Compute Engine.

Identity & Access

Access Approval: Access Approval allows customers to approve eligible manual, targeted accesses by Google administrators to their data or workloads before those accesses happen.

Access Context Manager: Access Context Manager allows Google Cloud organization administrators to define fine-grained, attribute based access control for projects, apps and resources.

BeyondCorp Enterprise: BeyondCorp Enterprise is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. BeyondCorp Enterprise is an integrated platform incorporating cloud-based services and software components, including:

- **On-premises Connector**, which forwards Identity-Aware Proxy traffic from Google Cloud Platform to applications and VMs deployed in non-Google Cloud Platform environments.
- **BCE app connector**, which provides secure access to private applications in non-Google cloud environments using a remote agent installed on a customer-owned virtual machine.
- **BCE client connector**, which provides end users secure access to private non-web applications using a remote endpoint agent installed on customer endpoint devices.
- **Endpoint Verification**, which allows administrators to build an inventory of devices and set the security posture of the devices.
- **Threat and Data Protection Services**, which are a set of security services that work by aggregating threat intelligence and are designed to protect enterprise users from malware transfers, phishing, malicious site visits, and sensitive data leakage.

- **BeyondCorp Enterprise Integration with Chrome Browser Cloud Management**, which enables malware, phishing, and data leakage protection for managed Chrome browsers.

- Other features listed at https://cloud.google.com/beyondcorp-enterprise/pricing or a successor URL.

Cloud Identity Services: Cloud Identity Services are the services and editions as described at: https://cloud.google.com/terms/identity/user-features.html or such other URL as Google may provide.

***Firebase Authentication**: Firebase Authentication provides a service as part of the Firebase platform to authenticate and manage users in your applications. It supports authentication using email & password, phone number and popular federated identity providers like Google and Facebook.

Google Cloud Identity-Aware Proxy: Google Cloud Identity-Aware Proxy is a tool that helps control access, based on a user's identity and group membership, to applications running on Google Cloud Platform.

Identity & Access Management (IAM): IAM provides administrators the ability to manage cloud resources centrally by controlling who can take what action on specific resources.

Identity Platform: Identity Platform provides you with functionality and tools to manage your users' identities and access to your applications. Identity Platform supports authentication and management of users with a variety of methods, including email & password, phone number, and popular federated identity providers like Google and Facebook.

Managed Service for Microsoft Active Directory (AD): Managed Service for Microsoft Active Directory is a Google Cloud service running Microsoft AD that enables you to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully-managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.

Resource Manager API: Resource Manager API allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization lets you easily manage common aspects of your resources such as access control and configuration settings.

Google Distributed Cloud

Google Distributed Cloud Edge: Google Distributed Cloud Edge allows you to run private Google Kubernetes Engine clusters on dedicated hardware, which is provided and maintained by Google on Customer premises.This solution also provides you with a VPN connection to Google Cloud Platform, allowing you to interact with other GCP Services or other applications running in your Virtual Private Cloud.

Sovereign Controls by Partners

Sovereign Controls by Partners: Sovereign Controls by Partners are solutions comprising a suite of Services offered by Google that are complemented by a set of services, offered by, and under separate terms of service with, third party partners ("**Sovereign Controls Partners**"), which together create additional security controls for certain Services, while also allowing the relevant Sovereign Controls Partner to provide additional security measures for those Services, as further described at: https://cloud.google.com/terms/in-scope-sovereign-cloud.

User Protection Services

reCAPTCHA Enterprise: reCAPTCHA Enterprise helps detect fraudulent activity on websites.

Web Risk API: Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

Serverless Computing

Cloud Run: Cloud Run (fully-managed) lets you run stateless containers on a fully-managed environment.

Cloud Functions: Cloud Functions is a lightweight, event-based, asynchronous compute solution that allows you to create small, single-purpose functions that respond to cloud events without the need to manage a server or a runtime environment.

***Cloud Functions for Firebase**: Cloud Functions for Firebase lets you write code that responds to events and invokes functionality exposed by other Firebase features, once you deploy JavaScript code in a hosted, private, and scalable Node.js environment that requires no maintenance.

Cloud Scheduler: Cloud Scheduler is a fully-managed enterprise-grade cron job scheduler. It allows you to schedule virtually any job, including batch, big data jobs, cloud infrastructure operations, and more. You can automate everything, including retries in case of failure to reduce manual toil and intervention. Cloud Scheduler even acts as a single pane of glass, allowing you to manage all your automation tasks from one place.

Cloud Tasks: Cloud Tasks is a fully-managed service that allows you to manage the execution, dispatch, and delivery of a large number of distributed tasks. Using Cloud Tasks, you can perform work asynchronously outside of a user or service-to-service request. Cloud Tasks provides all the benefits of a distributed task queue such as task offloading wherein heavyweight, background and long running processes can be dispatched to a task queue, loose coupling between microservices allowing them to scale independently, and enhanced system reliability as tasks are persisted in storage and retried automatically, making your infrastructure resilient to intermittent failures.

Eventarc: Eventarc is a fully-managed service for eventing on Google Cloud Platform. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).

Workflows: Workflows is a fully-managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs.

Internet of Things (IoT)

IoT Core: IoT Core is a fully-managed service that allows you to easily and securely connect, manage, and ingest data from internet connected devices. It permits utilization of other Google Cloud services for collecting, processing, analyzing, and visualizing IoT data in real time. IoT Core will be discontinued on August 16, 2023 and is not accepting new customers.

Management Tools

Google Cloud App: Google Cloud app is a native mobile app that enables customers to manage key Google Cloud services. It provides monitoring, alerting, and the ability to take actions on resources.

Cloud Deployment Manager: Cloud Deployment Manager is a hosted configuration tool which allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.

Cloud Shell: Cloud Shell is a tool that provides command-line access to cloud resources directly from your browser. You can use Cloud Shell to run experiments, execute Cloud SDK commands, manage projects and resources, and do lightweight software development via the built-in web editor.

Recommenders: Recommenders automatically analyze your usage patterns to provide recommendations and insights across services to help you use Google Cloud Platform in a more secure, cost-effective, and efficient manner.

Service Infrastructure: Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

- Service Management API, which lets service producers manage their APIs and services;
- Service Consumer Management API, which lets service producers manage their relationships with their service consumers; and
- Service Control API, which lets managed services integrate with Service Infrastructure for admission control and telemetry reporting functionality.
- Service Usage API, which lets service consumers manage their usage of APIs and services.

Healthcare and Life Sciences

Cloud Healthcare: Cloud Healthcare is a fully-managed service to send, receive, store, query, transform, and analyze healthcare and life sciences data and enable advanced insights and operational workflows using highly scalable and compliance-focused infrastructure.

***Healthcare Data Engine (HDE)**: HDE is a solution that enables (1) harmonization of healthcare data to the Fast Healthcare Interoperability Resources ("FHIR") standard and (2) streaming of healthcare data to an analytic environment.

Media and Gaming

Game Servers: Game Servers is a managed service that enables game developers to deploy and manage their dedicated game servers across multiple Agones clusters around the world through a single interface.

Live Stream API: Live Stream API is a cloud-based live encoder that processes high-quality contribution feeds for 24x7 live linear or live events and prepares the streams for digital distribution. It compresses the video and audio elementary streams with the latest video codecs and packages the streams in standardized container formats to reach all IP connected devices.

Transcoder API: Transcoder API can batch convert media files into optimized formats to enable streaming across web, mobile, and living room devices. It provides fast, easy to use, large-scale processing of advanced codecs while utilizing Google's storage, networking, and delivery infrastructure.

Video Stitcher API: Video Stitcher API enables users to dynamically insert content or ads using server-side video insertion technology. Video and ads are conditioned into a single stream for video on demand (VOD) or live streams to deliver flexible and target personalization at scale.

Google Cloud Platform Premium Software

Below is a list of available software components subject to the Google Cloud Platform Service Specific Terms as Premium Software.

Anthos: Anthos includes the following Premium Software components:

- **Anthos core software**: Anthos core software enables you to run containers on Kubernetes and can be deployed on premises in your own data center, as well as in both private and public clouds.

- **Anthos Service Mesh - Software**: Anthos Service Mesh - Software is a suite of tools to run a reliable service mesh on Anthos, to help you monitor, manage and secure traffic between the services deployed on Anthos.
- **Anthos Identity Service - Software**: Anthos Identity Service - Software may be downloaded and installed in supported cluster types and environments to let administrators set up authentication with their preferred Identity providers for one or more Anthos clusters.
- **Connect Software**: Connect Software may be downloaded and installed in clusters to enable connectivity between the customer-registered cluster and Google Cloud.
- **Cloud Logging and Cloud Monitoring for Anthos**: Cloud Logging and Cloud Monitoring can be deployed in a range of hybrid cloud environments to enable centralized log storage, log analysis, metrics capture, metrics trending, customized alerting, and application debug tracing.

***Apigee hybrid runtime**: Apigee hybrid runtime enables you to run the Apigee runtime plane in containers on Kubernetes within your data center.

***Apigee Private Cloud**: Apigee Private Cloud enables you to host and run Apigee entirely within your data center.

Cloud Vision OCR On-Prem: Cloud Vision OCR On-Prem enables you to run Cloud Vision OCR models within your data center and across multiple cloud environments.

Speech-to-Text On-Prem: Speech-to-Text On-Prem enables you to run Cloud Speech-to-Text models within your data center and across multiple cloud environments.

Google Cloud Platform Software

Below is a non-exclusive list of available software components subject to the Google Cloud Platform Service Specific Terms as Software.

- **BigQuery Connector for SAP** replicates, in connection with SAP Landscape Transformation Replication Server, SAP NetWeaver-based application data changes in near real-time and directly into BigQuery.
- **Cloud Run for Anthos deployed on VMware** enables you to run stateless containers on VMware.
- **Config Connector** is a Kubernetes add-on that allows you to manage your Google Cloud resources through Kubernetes configuration files.
- **Google Cloud SDK**: Google Cloud SDK is a set of tools to manage resources and applications hosted on Google Cloud Platform. It includes the Google Cloud Command Line Interface (CLI), Cloud Client Libraries for programmatic access to Google Cloud Platform services, the gsutil, kubectl, and bq command line tools, and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to Google Cloud Platform.
- **Kf** enables you to migrate and run applications from the open-source Cloud Foundry platform into containers in Google Kubernetes Engine and Anthos.
- **Migrate to Containers** enables you to migrate and run applications from virtual machines on-premise or other clouds into containers in Google Kubernetes Engine, Anthos, and Cloud Run, while producing container and data artifacts for integration with modern CI/CD, Anthos and Google Cloud services. Migrated container images and artifacts are portable for use across a variety of Google Kubernetes Engine, Anthos, and Cloud Run hybrid configurations as listed in the applicable software documentation. With Migrate to Containers, the need for application rewrite is minimized.
- **Migrate for Compute Engine v4.X** enables you to validate, run, and migrate applications from on-premise or other clouds into Compute Engine while minimizing downtime and application rewrite.

PREVIOUS VERSIONS *(Last modified December 13, 2022)*

Google Cloud Platform Key Services

The following are excluded from this list: (i) specific resource and instance types; (ii) specific programming languages and add-on tools; (iii) open source or third-party components or software; and (iv) any versions, features, or functionality that are pre-general availability.

Storage & Compute Services:

- App Engine
    - Excluding APIs for Mail, Images, and Blobstore
- BigQuery
- Cloud Bigtable
- Cloud Spanner
- Cloud SQL
- Cloud Storage
- Compute Engine
- Dataflow
- Dataproc
- Firestore
- Google Kubernetes Engine
- Persistent Disk

Google Cloud Platform Networking Services:

- Cloud DNS
- Cloud Interconnect
- Cloud Load Balancing
- Virtual Private Cloud (VPC)
- VPC Service Controls

Other Google Cloud Platform Services and Software:

- Anthos (the following management Services only):
    - Anthos Config Management
    - Connect
    - Hub
- Cloud Healthcare
- Cloud SDK
- Identity & Access Management (IAM)

Google Cloud Platform Services: Technical Support Services Guidelines

These technical support services guidelines ("Guidelines") are incorporated into the agreement under which Google has agreed to provide Google Cloud Platform and related technical support (as described at https://cloud.google.com/terms/services) to Customer (the "Agreement"). Capitalized terms used but not defined in the Guidelines have the meaning given to them in the Agreement.

Regardless of any other statement in the Agreement or these Guidelines, Google does not offer Technical Support Services ("TSS") to Customer for Cloud Identity or Looker Studio (except for Looker Studio Pro). For Cloud Identity Google will instead provide Customer support in accordance with the Cloud Identity Technical Support Services Guidelines (available at https://cloud.google.com/terms/identity/tssg). Google offers Customer support for the Looker Platform Services (as defined in the Looker Platform Support Services Guide) in accordance with the Looker Support Services Guide (available at https://cloud.google.com/terms/tssg/looker). Google offers TSS to Customer for Firebase services, except as described in the Firebase Technical Support Services Guide (available at https://cloud.google.com/terms/tssg/firebase/). Google offers TSS to Customer for Apigee, except as described in the Apigee Support Services Guide (available at https://cloud.google.com/terms/apigee-support-services-guide) and for Apigee Edge, TSS is offered in accordance with the Apigee Technical Support Services Guidelines (available at https://cloud.google.com/terms/apigee-support).

Collapse all

General Support Services Terms

1. **Generally.** As part of Customer's purchase of Google Cloud Platform Services, Google will provide Basic (formerly Bronze) Support to Customer. Customer may order additional TSS for an additional fee.

2. **Basic Support.** Customer will receive automatic Services upgrades and Maintenance updates, support for billing inquiries, and access to documentation, white papers, online best practices guides, and community forums.

3. **Support Request Submission.**

3.1. *First Line Support*. Customer will provide first-level support to Customer End Users. Google will provide second-level support to Customer's Designated Contacts only.

3.2. *Customer Efforts to Fix Errors*. Prior to making a request to Google, Customer will use reasonable efforts to fix any error, bug, malfunction or network connectivity defect without escalation to Google. Thereafter, Customer may submit a Request for TSS.

3.3. *Characterization of Requests*. Customer designates P1-P4 priority upon submission of Requests. Google will review Customer's priority designation and may reclassify designations (a) that Google believes are incorrect or (b) where Customer fails to maintain continuous availability, as described in Section 3.4 (Procedures for Acknowledgement and Resolution of Requests) through the resolution of a Request. Any such determination made by Google is final and binding on Customer. Any reclassification by Google of the Priority designation pursuant to subsection (b) will be reversed once Customer resumes continuous availability with Google in accordance with Section 3.4 (Procedures for Acknowledgement and Resolution of Requests).

3.4. *Procedures for Acknowledgement and Resolution of Requests*. When making a Request, Customer will provide all requested diagnostic information and assist Google Support Personnel as may be required to resolve a Request. Customer must provide up-to-date contact information (i.e., phone or email) to assist with data gathering, testing and applying resolutions. In the case of P1 Requests, Customer must maintain continuous availability until resolution of such Requests. Upon resolution of a Request, Customer may receive an optional survey to provide feedback to Google on the support Request experience.

3.5. *Request Acknowledgement*. Google may respond to a Request by acknowledging receipt of the Request. Customer acknowledges and understands that Google may be unable to provide answers to, or resolve all Requests.

3.6. *Feature Requests*. If Google deems a Request to be a Feature Request, Google will log such Request for consideration to add to a future update or release of the Services and will consider the matter closed. Google is under no obligation to respond to or resolve any Feature Request or to include any such Feature Request in any future update or release.

3.7. *Building Applications*. For clarity, Google has no obligation under these Guidelines to: (a) write, build or improve any software Applications, or write code to facilitate Applications; (b) configure the Services for Customer; or (c) design, build or review Customer infrastructure.

3.8. *Pre-General Availability Offerings*. Google has no obligation to provide TSS for Pre-GA Offerings, but will consider Requests relating to Pre-GA Offerings on a case-by-case basis.

4. **Accessing Support.**

4.1. *Setting Designated Contacts*. Customer-designated support admins may add Designated Contacts to its Account. Solely with respect to Silver, Gold, and Platinum TSS, if Customer wishes to change its Designated Contacts, it will notify Google via the Google Support Tool at least five Business Days prior to the change, as applicable.

4.2. *Support Hours and Target Initial Response Times*. Google will process Requests during the Hours of Operation and in accordance with the applicable target initial response times for each support level, unless otherwise indicated in these Guidelines. Any Requests received outside of the Hours of Operation will be logged and processed during the next Business Day.

4.3. *Compliance with Applicable Law.* Google will not provide TSS if prohibited from doing so by applicable law.

5. **Maintenance.** To ensure optimal performance of the Services, Google performs periodic Maintenance. In most cases, Maintenance will have limited or no negative impact on the availability and functionality of the Services. If Google expects planned Maintenance to negatively affect the availability or functionality of the Services, Google will use commercially reasonable efforts to provide at least seven days' advance notice of the Maintenance. In addition, Google may perform emergency unscheduled Maintenance at any time. If Google expects such emergency unscheduled Maintenance to negatively affect the availability or functionality of the Services, Google will use commercially reasonable efforts to provide advance notice of such Maintenance. Maintenance notices noted above will be provided via the Google Support Tool or via an email to the Notification Email Address.

6. **Language Support.** All support provided by Google pursuant to these Guidelines will be provided in the English language except as provided at https://cloud.google.com/support/docs/language-working-hours.

7. **Support Data Processing Activities.** Google collects and processes Support Data for the purpose of providing TSS under these Guidelines and maintaining the Services.

8. **Technical Account Management (TAM).** As part of the Platinum, Enterprise and Premium Support offerings, Customer will receive access to a named Technical Account Manager to: (a) assist Customer in developing a strategy with respect to the Services, (b) provide best practice guidance on implementation and use of the Services, and (c) manage technical support escalations and coordinate with Google subject matter experts to address technical inquiries related to the Services. Additional access to Technical Account Management may be purchased, subject to additional fees and terms.

9. **Professional Services.** In addition to the support and maintenance services described above, Google may provide limited advisory services to Customer under these Guidelines in accordance with an order form executed by Google and Customer and datasheets associated with the services. Additional fees may apply. Advisory services are recommendations only. Customer is responsible for the results achieved when determining whether to implement recommendations from Google. Google may deliver recommendations to Customer in the form of a working paper or report, which Customer may use, modify and reproduce for its internal business purposes. Google will not otherwise license any intellectual property to Customer as part of the advisory services provided under these Guidelines. Any other advisory, professional or implementation services will be subject to the terms of a separate agreement between Google and Customer.

10. **Collaborative Support.** In recognition that Customer may deploy and use Services that are offered in connection with or that rely upon a range of third party hardware and software components and computing platforms, resolving Requests may sometimes require input from third party providers who have qualified to participate in the Google Cloud Platform collaborative support program (such providers, "Collaborative Support

Partners"). Google will, in its reasonable determination, identify to Customer any Requests that require the involvement of Collaborative Support Partner(s). Google may include Collaborative Support Partners in support communications with Customer, subject to the following terms:

10.1. Customer may only receive support from a Collaborative Support Partner if Customer has a valid support agreement in place with that Collaborative Support Partner. Neither these Guidelines nor the Agreement grant to Customer any right to receive support services from Collaborative Support Partners.

10.2. Google will include Collaborative Support Partners in direct support communications with Customer solely at Customer's direction. Google Support Personnel will only reach out to a Collaborative Support Partner after receiving Customer's consent.

10.3. When Customer consents to include a Collaborative Support Partner in an ongoing support case, Customer consents to Google providing that Collaborative Support Partner with Support Data Google reasonably deems relevant to the Request, including Customer's name, contact information, and a description of the Request. When Customer directs Google to engage a Collaborative Support Partner, the Collaborative Support Partner acts as an independent contractor of the Customer, not Google. The Collaborative Support Partner, not Google, is solely responsible for the processing and use of any information, including Support Data, provided to that Collaborative Support Partner in the course of providing support services.

11. **Resold Customer.** A customer (a "Resold Customer") of a Google-authorized unaffiliated Google Cloud Platform reseller (a "Reseller") may purchase Google-supplied technical support services that are approved and enabled for resale through the Reseller ("Resold TSS"), provided that:

11.1. the prices and fees for Resold TSS, and the terms applicable to Resold Customer's use of Resold TSS, are agreed as between Resold Customer and the Reseller;

11.2. any payment for Resold TSS is made directly to Reseller under Resold Customer's applicable agreement with the Reseller; and

11.3. Google will not provide Resold Customer any billing inquiry support on the Services.

12. **Chrome Support**. If Customer purchases Enhanced or Premium Support then Google Support Personnel will also respond to Requests related to Chrome installation, Chrome Core Functionality, Chrome's security and administrative policies, and Chrome's interoperability with Services on Supported Platforms as set forth in these Guidelines. Google may choose not to respond to Requests for other Chrome related technical issues, such as but not limited to, rendering problems for specific web pages, technical issues related to the underlying operating system, device driver or printer problems. If Google makes a code change to Chrome to resolve a technical issue, that code change will be released in an upcoming release and will not be ported back to an earlier version of Chrome.

13. **Additional Definitions.**

13.1. *"Application"* has the meaning given in the Agreement or, if not such meaning is given, has the meaning given to "Customer Application" in the Agreement.

13.2. *"Business Day"* means any day during the Hours of Operation.

13.3. *"Chrome"* means the Chrome web browser as released by Google for Supported Platforms and available for download at the URL https://www.google.com/chrome/ or the installer provided at the URL https://chromeenterprise.google/browser/ or at another URL that Google may provide.

13.4. *"Chrome Core Functionality"* means the features and functionality in the latest released Chrome browser version, excluding Google Chrome extensions, and Google Play.

13.5. *"Customer End User"* has the meaning given in the Agreement or, if no such meaning is given, has the meaning given to "End Users" in the Agreement.

13.6. "*Designated Contacts"* means administrators or technical employees designated by Customer or Reseller (if Customer is accessing TSS as a customer of a Reseller) who are allowed to contact Google for technical support.

13.7. *"Feature Request"* means a Request by a Designated Contact to incorporate a new feature or enhance an existing feature of the Services that is currently not available as part of the existing Services.

13.8. *"Google Support Tool"* means the Admin Console or a support tool located at a URL (as may be updated from time to time) provided by Google.

13.9. *"Google Support Personnel"* means the Google representatives responsible for handling Requests.

13.10. *"Hours of Operation"* means 17:00 on Sunday to 17:00 on Friday Pacific Time Zone, except for holidays in local time for each region documented in the Google Support Tool.

13.11. *"Maintenance"* means maintenance work that is performed on hardware or software delivering the Services.

13.12. *"Notification Email Address"* has the meaning given in the Cloud Data Processing Addendum.

13.13. *"P0"* means impact to operating environments that have been provisioned to support Mission Critical Services.

13.14. *"P1"* means Critical Impact – Service Unusable in Production.

13.15. *"P2"* means High Impact – Service Use Severely Impaired.

13.16. *"P3"* means Medium Impact – Service Use Partially Impaired.

13.17. "P4" means Low Impact – Service Fully Usable.

13.18. *"Priority"* means P0, P1, P2, P3 or P4 depending on the level of impact a Request is having on Customer's operations and is used to establish initial target response times.

13.19. *"Request"* means a request from a Designated Contact to Google Support Personnel for technical support to resolve a question or problem report regarding the Services, Chrome, or Chrome Core Functionality, as applicable.

13.20. *"Reseller"* has the meaning given to it in Section 11 (Resold Customer) in the General Support Service Terms of these Guidelines.

13.21. *"Support Data"* means account details and the information that Customer provides to Google for the purpose of obtaining TSS under these Guidelines, including requests for support and the details provided to Google about the specific support issue.

13.22. *"Support Role"* means the level of support available to a Designated Contact under Role-Based Support, as defined by one of two tiers (Development or Production) and as designated by Customer in accordance with Section 1 (Support Roles) of the Role-Based Support terms.

13.23. *"Supported Platform"* means an operating system and version listed at https://support.google.com/a/bin/answer.py?answer=2763059 for which Chrome is released by Google. Google may choose not to respond to issues with preview versions of Chrome (also known as beta, dev, and canary) or preview features. Chrome OS is not a Supported Platform under these Guidelines; dedicated Google technical support and hardware service for Chrome OS is available under a separate agreement. For clarity, Chrome Frame is a separate product not covered under these Guidelines.

13.24. *"Value Add Services"* means additional TSS available to Customer for an additional fee.

Standard Support

1. **Standard Support.** Standard Support includes unlimited Designated Contacts.

2. **Target Initial Response Times for Standard Support.**

Priority	Target Initial Response Times during the Hours of Operation
P1	N/A
P2	4 hours
P3	8 hours
P4	8 hours

3. **Enrollment and Unenrollment of Standard Support.**

3.1 Standard Support requires a minimum commitment through the end of each calendar month.

3.2 Customer may unenroll from Standard Support through the Google Support Tool, in which case Basic Support will apply after the end of the calendar month. If Customer upgrades from Standard Support, the applicable Fees for the new support level will be calculated from the date of such upgrade.

Enhanced Support

1. **Enhanced Support**

1.1. Enhanced Support includes unlimited Designated Contacts.

1.2. *Value Add Services*. Customer may purchase the following Value Add Services for an additional fee:

1.2.1. *Technical Account Advisor Service (TAAS)*. Customer will receive access to a Technical Account Advisor. TAAS includes: (a) guided support onboarding, (b) guidance on best practices for case handling, (c) management of technical support escalations, (d) reviews of operational and case metrics, and (e) recommendations for training and optimization of the Services.

1.2.2. *Assured Support for Enhanced Support*. Google will provide TSS for Assured Workloads ("Assured Support") in accordance with the Customer-selected Admin Console controls. All Requests for Assured Support by Customer must be submitted via the "create case" option from within the Google Support Tool and include the project name (ID) in the project field, which corresponds to an Assured Workloads project. Google will provide Assured Support in the English language only.

1.2.3. *Planned Event Support (PES)*. If Customer wishes to purchase PES for an event, it must do so no less than 30 days before that event to ensure proper planning. Each event is limited to a maximum of five calendar days. During each event, regardless of Section 2 (Target Initial Response Times for Enhanced Support) below, Google will respond to P1 Requests that are related to the event with a target initial response time of 15 minutes. Customer can purchase PES for up to three events per calendar year.

1.2.4. *Sovereign Controls by Partners Support for Enhanced Support.* If (i) Customer is using Sovereign Controls by Partners; (ii) the Sovereign Controls Partner does not provide technical support for Sovereign Controls by Partners; and (iii) Customer has purchased Enhanced Support, then Google will provide TSS for the In-scope Google Cloud Controls defined in the Service Specific Terms ("Sovereign Controls by Partners Support") in accordance with the Customer-selected security controls in the Admin Console. All Requests for Sovereign Controls by Partners Support must be submitted via the "create case" option from within the Google Support Tool and include the Project name (ID) in the Project field, which corresponds to a Sovereign Controls by Partners Project with the relevant Sovereign Controls Partner. Google will provide Sovereign Controls by Partners Support in the English language only.

2. **Target Initial Response Times for Enhanced Support.**

Priority	Target Initial Response Times
P1	1 hour
P2	4 hours
P3	8 hours*
P4	8 hours*

*during the Hours of Operation

3. **Enrollment and Unenrollment of Enhanced Support.**

3.1. Enhanced Support requires a minimum commitment through the end of each calendar month or as described in the applicable Order Form.

3.2. Customer may unenroll from Enhanced Support by notifying Google in writing or through the Google Support Tool, as applicable, in which case Basic Support will apply after the end of the applicable commitment period. If Customer enrolls in another support level other than Basic Support, the applicable Fees for the new support level will be calculated from the date of such new enrollment.

Premium Support and Partner-Led Premium Support

1. **Premium Support.**

1.1. Premium Support includes unlimited Designated Contacts.

1.2. Premium Support includes support from Google's Technical Account Management, as described in Section 8 of the General Support Services Terms (Technical Account Management).

1.3. *Value Add Services*. Customer may purchase the following Value Add Services for Premium Support for an additional fee:

1.3.1. *Assured Support for Premium Support*. Google will provide TSS for Assured Workloads ("Assured Support") in accordance with the Customer-selected Admin Console controls. All Requests for Assured Support by Customer must be submitted via the "create case" option from within the Google Support Tool and include the project name (ID) in the project field, which corresponds to an Assured Workloads project. Google will provide Assured Support in the English language only.

1.3.2. *Mission Critical Services (MCS)*. Google will provide a target initial response time of 5 minutes for P0 cases for operating environments that have been provisioned to support MCS, as noted in the table in Section 3 (Target Initial Response Times for Premium Support and Partner-Led Premium Support). Google will provide TSS for MCS in the English language only.

1.3.3. *Sovereign Controls by Partners Support for Premium Support.* If (i) Customer is using Sovereign Controls by Partners; (ii) the Sovereign Controls Partner does not provide technical support for Sovereign Controls by Partners; and (iii) Customer has purchased Premium Support, then Google will provide TSS for the In-scope Google Cloud Controls defined in the Service Specific Terms ("Sovereign Controls by Partners Support") in accordance with the Customer-selected security controls in the Admin Console. All Requests for Sovereign Controls by Partners Support by Customer must be submitted via the "create case" option from within the Google Support Tool and include the Project name (ID) in the Project field, which corresponds to a Sovereign Controls by Partners Project with the relevant Sovereign Controls Partner. Google will provide Sovereign Controls by Partners Support in the English language only.

2. **Partner-Led Premium Support.**

2.1. Partner-Led Premium Support includes unlimited Designated Contacts.

2.2. *Partner Operations Management (POM)*. As part of the Partner-Led Premium Support offering, Customer will receive access to a named Partner Operations Manager. POM includes: (a) assistance in developing a cloud strategy with respect to the Services, (b) best practices guidance on implementing and using the Services, and (c) management of technical support escalations and coordination with Google subject matter experts to address technical inquiries related to the Services.

3. **Target Initial Response Times for Premium Support and Partner-Led Premium Support.**

Priority	Target Initial Response Times
P0	5 minutes (Premium Support with MCS only)
P1	15 minutes
P2	2 hours

Priority	Target Initial Response Times
P3	4 hours*
P4	8 hours*

*during the Hours of Operation

4. **On-Site Support for Premium Support and Partner-Led Premium Support.** Google may, at its discretion and with Customer's approval, send Google Support Personnel on-site in response to an issue that cannot be resolved remotely. Google Support Personnel performing support at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.

5. **Enrollment and Unenrollment of Premium Support and Partner-Led Premium Support.**

5.1. Premium Support and Partner-Led Premium Support requires a minimum 1-year Fee commitment from the date on which Customer enrolls.

5.2. Customer may unenroll from Premium Support or Partner-Led Premium Support at any time by notifying Google in writing and any such unenrollment will take effect, and applicable Fees for Customer's downgraded support level will be calculated at the downgraded amount, from the later of (a) the date of such unenrollment, and (b) the Business Day following the 1-year anniversary of Customer's enrollment in Premium Support or Partner-Led Premium Support. Unenrollment from Premium Support automatically unenrolls all Value Add Services.

5.3. Sections 5.1 and 5.2 above will not apply if Customer is an existing Platinum or Enterprise Support customer. Instead, the minimum term of Customer's current Platinum or Enterprise Support Order Form will govern its use of Premium Support or Partner-Led Premium Support until the expiration of such Order Form.

[Legacy] Silver, Gold and Platinum Support

1. **Silver.** The Silver support level includes all the items in Basic Support plus the ability to submit support Requests for questions about Services functionality, best practice guidance on how to architect with the Services, and Services errors reports, as well as up to two Designated Contacts.

2. **Gold.** The Gold support level includes all the items in the Silver level plus consultation on application development, and specific guidance on how to architect with the Services for Customer's proposed use case, as well as up to five Designated Contacts.

3. **Platinum.** The Platinum support level includes all the items in the Gold level plus Unlimited Designated Contacts and access to Google's Technical Account Management team as described in the General Support Service Terms Section 8 (Technical Account Management).

4. **Target Initial Response Times for Silver, Gold and Platinum Support.**

Priority	Target Initial Response Times		
	Silver	Gold	Platinum
P1	4 hours*	1 hours	15 minutes
P2	8 hours*	4 hours*	4 hours*
P3	8 hours*	8 hours*	8 hours*
P4	8 hours*	8 hours*	8 hours*

*during the Hours of Operation

5. **Priority Designations.** Notwithstanding Section 3.3 (Characterization of Requests) of the General Support Services Terms of these Guidelines, Google will inform Customer of any change of Customer's Priority designation in its response to the support Request. Customer may appeal any such reclassification to Google's Support management for review through any available support channel.

[Legacy] Role-Based Support

1. **Support Roles.** Google will provide Customer with technical support through its Designated Contacts, according to their designated Support Role as follows:

    1.1. *Development*. The Development Support Role includes all the items in Basic Support plus the ability to submit Requests related to Services functionality, best practices guidance on how to architect with the Services, and Services errors reports.

    1.2. *Production*. The Production Support Role includes all the items in the Development Support Role plus limited guidance on how to architect with the Services for Customer's proposed use case.

2. **Target Initial Response Times for Role-Based Support.**

Priority	Target Initial Response Times	
	Development	Production
P1	N/A	1 hour
P2	4 hours*	4 hours*
P3	8 hours*	8 hours*
P4	8 hours*	8 hours*

*during the Hours of Operation

3. **Upgrading/Downgrading Support Roles in Role-Based Support.** All Support Roles require a minimum 30-day Fee commitment.

    3.1. *Upgrades*. Customer may designate or upgrade a Support Role for a Designated Contact at any time. When Customer designates or upgrades any Support Role for a Designated Contact, any applicable Fees will be pro-rated in that month, and will automatically renew at the beginning of the following month. Customer may upgrade a Support Role for a Designated Contact at any time. Any applicable Fees for such upgraded Support Role will be calculated at the upgraded rate beginning on the day that the upgrade is processed.

    3.2. *Downgrades*. Customer may downgrade or remove a Support Role for a Designated Contact at any time. Such downgrade or removal will take effect, and any applicable Fees for such downgraded or removed Support Role will be calculated at the downgraded amount, from the later of (a) the date of such downgrade or removal, and (b) 30 days after the Support Role for the Designated Contact was last changed, and the applicable Fees will automatically renew at the beginning of the month following such downgrade or removal.

[Legacy] Enterprise Support

1. **Enterprise Support.**

    1.1. The Enterprise Support offering includes unlimited Designated Contacts, each with Customer's chosen Support Role. The "Business Critical" level of support is only available to Customers who have enrolled in Enterprise Support.

1.2. If enrolled in the Enterprise Support program, Customer may assign the "Business Critical" role to each of its unlimited Designated Contacts.

2. **Target Initial Response Times for Enterprise Support.**

Priority	Target Initial Response Times during the Hours of Operation
P1	15 minutes 24x7
P2	4 hours 24x7
P3	8 hours
P4	8 hours

3. The Enterprise Support offering includes support from Google's Technical Account Management, as described in Section 8 of the General Support Services Terms (Technical Account Management).

4. **On-Site Support.** Google may, at its discretion and with Customer's approval, send Google Support Personnel on-site in response to an issue that cannot be resolved remotely. Google Support Personnel performing support at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.

5. **Enrollment and Unenrollment.**

5.1. The Enterprise Support program requires a minimum 1-year Fee commitment from the date on which Customer enrolls.

5.2. Customer may unenroll from the Enterprise Support program at any time by notifying Google in writing and any such unenrollment will take effect, and applicable Fees for Customer's downgraded Support Role(s) will be calculated at the downgraded amount, from the later of (a) the date of such unenrollment, and (b) the Business Day following the 1-year anniversary of Customer's enrollment in Enterprise Support.

5.3. Sections 5.1 and 5.2 above will not apply if Customer is an existing Platinum Support customer. Instead of Customer's current Platinum Support Order Form will govern its use of Enterprise Support until the expiration of such Order Form.

Back to Google Cloud Terms Directory (https://cloud.google.com/product-terms) > Current

Google Cloud Platform Acceptable Use Policy

Use of the Services is subject to this Acceptable Use Policy.

Capitalized terms have the meaning stated in the applicable agreement between Customer and Google.

Customer agrees not to, and not to allow third parties to use the Services:

- to violate, or encourage the violation of, the legal rights of others (for example, this may include allowing Customer End Users to infringe or misappropriate the intellectual property rights of others in violation of the Digital Millennium Copyright Act);
- to engage in, promote or encourage illegal activity;
- for any unlawful, invasive, infringing, defamatory or fraudulent purpose (for example, this may include phishing, creating a pyramid scheme or mirroring a website);
- to intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
- to disable, interfere with or circumvent any aspect of the Services;
- to generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisings or other solicitations ("spam"); 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.

PREVIOUS VERSIONS *(Last modified December 16, 2015)*

September 18, 2012 _ (/terms/aup-20120918)

Back to Google Cloud Terms Directory (/product-terms) > Current

Cloud Data Processing Addendum (Customers)

This Cloud Data Processing Addendum including its appendices ("*Addendum*") is incorporated into the Agreement(s) under which Google has agreed to provide Google Cloud Platform, Google Workspace, or Cloud Identity (each as defined below), as applicable (the "*Services*"), to Customer. This Addendum was formerly known as the "Data Processing and Security Terms" under an Agreement for Google Cloud Platform and the "Data Processing Amendment" under an Agreement for Google Workspace or Cloud Identity.

1. Commencement

This Addendum will be effective and replace any terms previously applicable to the processing of Customer Data, including any Data Processing and Security Terms or Data Processing Amendment, from the Addendum Effective Date (as defined below).

2. Definitions

2.1 Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement:

- *Account* has the meaning given in the applicable Agreement or, if no such meaning is given, means Customer's Google Cloud Platform account, Google Workspace account or Cloud Identity account, as applicable.
- *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/or controls that Customer may use at its option and/or as it determines, including the Admin Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- *Adequate Country* means:

  (a) for data processed subject to the EU GDPR: the EEA, 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; and/or

(c) for data processed subject to the Swiss FDPA: 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, or (ii) recognized as ensuring adequate protection by the Swiss Federal Council under the Swiss FDPA;

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

- *Alternative Transfer Solution* means 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.
- *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 (/security/compliance/services-in-scope). Google may not remove any Services from this URL unless those Services have been discontinued in accordance with the applicable Agreement.
- *Cloud Identity* means the Cloud Identity Services described at https://cloud.google.com/terms/identity/user-features (/terms/identity/user-features), when purchased under a standalone Agreement.
- *Customer Data* has the meaning given in the applicable Agreement or, if no such meaning is given, means:

  (a) data provided by or on behalf of Customer or its End Users via Google Cloud Platform under the Account; or

  (b) 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.
- *Customer Personal Data* means the personal data contained within the Customer Data, including any special categories of personal data defined under European Data Protection Law.
- *Customer SCCs* means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Processor) and/or the SCCs (Processor-to-Controller), as applicable.
- *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.
- *EEA* means the European Economic Area.
- *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; and/or (b) the Swiss FDPA.

- *European Law* means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).
- *GDPR* means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.
- *Google Cloud Platform* means the Google Cloud Platform services described at https://cloud.google.com/terms/services (https://cloud.google.com/terms/services), excluding any Third-Party Offerings.
- *Google Workspace* means the Google Workspace or Google Workspace for Education services described at https://workspace.google.com/terms/user_features.html (https://workspace.google.com/terms/user_features.html), as applicable.
- *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 5.2.1 (Compliance with Customer's Instructions).
- *Non-European Data Protection Law* means data protection or privacy laws in force outside the EEA, the UK and Switzerland.
- *Notification Email Address* means the email address(es) designated by Customer in the Admin Console or Order Form to receive certain notifications from Google. Customer is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.
- *SCCs* means the Customer SCCs and/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 (https://cloud.google.com/terms/sccs/eu-c2p)
- *SCCs (Processor-to-Controller)* means the terms at: https://cloud.google.com/terms/sccs/eu-p2c (https://cloud.google.com/terms/sccs/eu-p2c)
- *SCCs (Processor-to-Processor)* means the terms at: https://cloud.google.com/terms/sccs/eu-p2p (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 (https://cloud.google.com/terms/sccs/eu-p2p-google-exporter)
- *Security Documentation* means all documents and information made available by Google under Section 7.5.1 (Reviews of Security Documentation).
- *Security Measures* has the meaning given in Section 7.1.1 (Google's Security Measures).
- *Subprocessor* means a third party authorized as another processor under this Addendum to have logical access to and process Customer Data in order to provide parts of the Services and TSS.

- *Supervisory Authority* means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; and/or (b) the "Commissioner" as defined in the UK GDPR and/or the Swiss FDPA.
- *Swiss FDPA* means the Federal Data Protection Act of 19 June 1992 (Switzerland).
- *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 in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

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. Scope of Data Protection Law

4.1 *Application of European Law*. The parties acknowledge that European Data Protection Law will apply to the processing of Customer Personal Data if, for example:

a. the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA or the UK; and/or

b. the Customer Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services in the EEA or the UK, or the monitoring of their behavior in the EEA or the UK.

4.2 *Application of Non-European Law*. The parties acknowledge that Non-European Data Protection Law may also apply to the processing of Customer Personal Data.

4.3 *Application of Addendum*. Except to the extent this Addendum states otherwise, this Addendum will apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

5. Processing of Data

5.1 *Roles and Regulatory Compliance; Authorization*.

5.1.1 *Processor and Controller Responsibilities*. If European Data Protection Law applies to the processing of Customer Personal Data:

a. the subject matter and details of the processing are described in Appendix 1;

b. Google is a processor of that Customer Personal Data under European Data Protection Law;

c. Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Law; and

d. each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of that Customer Personal Data.

5.1.2 *Processor Customers*. If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor:

a. Customer warrants on an ongoing basis that the relevant controller has authorized: (i) the Instructions, (ii) Customer's appointment of Google as another processor, and (iii) Google's engagement of Subprocessors as described in Section 11 (Subprocessors);

b. Customer will immediately forward to the relevant controller any notice provided by Google under Sections 5.2.2 (Instruction Notifications), 7.2.1 (Incident Notification), 9.2.1 (Responsibility for Requests), 11.4 (Opportunity to Object to Subprocessor Changes) or that refers to any SCCs; and

c. Customer may:

i. request access for the relevant controller to the SOC Reports in accordance with Section 7.5.3(a); and

ii. make available to the relevant controller any other information made available by Google under Sections 10.4 (Supplementary Measures and Information), 10.6 (Data Center Information) and 11.2 (Information about Subprocessors).

5.1.3 *Responsibilities under Non-European Law.* If Non-European Data Protection Law applies to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

5.2 *Scope of Processing*.

5.2.1 *Compliance with Customer's Instructions*. Customer instructs Google to process Customer Data in accordance with the applicable Agreement (including this Addendum) and applicable law only: (a) to provide, secure, and monitor the Services and TSS; and (b) as further specified via (i) Customer's use of the Services (including the Admin Console and other Services functionality) and TSS, 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.

5.2.2 *Instruction Notifications*. Without prejudice to Google's obligations under Section 5.2.1 (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.

5.3 *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.

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 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.

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 in accordance with applicable law. 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.

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 (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 relevant controller's) obligations under Articles 32 to 34 of the GDPR, 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 to Customer in accordance with Section 7.1.3 (Additional Security Controls);

c. complying with the terms of Section 7.2 (Data Incidents);

d. providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement (including this Addendum); and

e. if subsections (a)-(d) above are insufficient for Customer (or the relevant 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 *Delivery of Notification*. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address.

7.2.4 *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.

7.2.5 *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 implemented and maintained by Google, 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 Personal 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 in order to evaluate the continued effectiveness of the Security Measures: (a) certificates for ISO 27001, ISO 27017 and ISO 27018 and, for Google Cloud Platform, a PCI DSS Attestation of Compliance (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*. Google will make the Compliance Certifications and the SOC Reports available for review by Customer to demonstrate compliance by Google with its obligations under this Addendum.

7.5.2 *Customer's Audit Rights*.

a. If European Data Protection Law applies to the processing of Customer Personal Data, Google will 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 make available all information necessary to demonstrate such compliance and contribute to the audit as described in Section 7.4 (Compliance Certifications and SOC Reports) and this Section 7.5 (Reviews and Audits of Compliance).

b. If Customer SCCs apply as described in Section 10.2 (Restricted European 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).

c. 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 send any requests for reviews of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1, or audits under Section 7.5.2(a) or 7.5.2(b), to Google's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).

b. Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1; 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) or 7.5.2(b).

c. Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) or 7.5.2(b). 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) or 7.5.2(b) 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.

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 relevant controller's) obligations under Articles 35 and 36 of the GDPR, by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation 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 relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

9. Access etc.; 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 European Data Protection 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 relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:

a. providing Additional Security Controls 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 relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

10. Data Transfers

10.1 *Data Storage and Processing Facilities*. Subject to Google's data location commitments under the Service Specific Terms and the remainder of this Section 10 (Data Transfers), Customer Data may be

processed in any country in which Google or its Subprocessors maintain facilities.

10.2 *Restricted European 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 10.3 (Certification by Non-EMEA Customers) if its billing address is outside EMEA) ("*Restricted European Transfers*"), then:

a. if Google has adopted an Alternative Transfer Solution for any Restricted European Transfers, then Google will inform Customer of the relevant solution and ensure that such Restricted European Transfers are made in accordance with it; and/or

b. if Google has not adopted, or informs Customer that Google is no longer adopting, an Alternative Transfer Solution for any Restricted European Transfers, then:

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 European 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 and/or processor) with respect to such Restricted European Transfers between Google and Customer; or

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

10.3 *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, Customer will certify as such, and identify its competent Supervisory Authority, via the Admin Console for Google Cloud Platform or Google Workspace and Cloud Identity, as applicable.

10.4 *Supplementary Measures and Information*. Google will provide Customer with information relevant to Restricted European Transfers, including information about Additional Security Controls and other supplementary measures to protect Customer Personal Data:

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

b. in the documentation for the Services, available at https://cloud.google.com/docs (https://cloud.google.com/docs); and

c. in the Google Cloud Trust and Security website, available at https://cloud.google.com/security (/security).

10.5 *Termination*. If Customer concludes, based on its current or intended use of the Services, that the Alternative Transfer Solution and/or SCCs, as applicable, do not provide appropriate safeguards for Customer Personal Data, then Customer may immediately terminate the applicable Agreement for convenience by notifying Google.

10.6 *Data Center Information*. The locations of Google data centers are described at:

a. https://cloud.google.com/about/locations/ (https://cloud.google.com/about/locations/) for Google Cloud Platform; and

b. https://www.google.com/about/datacenters/locations/ (https://www.google.com/about/datacenters/locations/?_ga=2.51070953.1907356626.1655412346-310495072.1655412346) for Google Workspace and Cloud Identity.

11. Subprocessors

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

11.2 *Information about Subprocessors*. Names, locations and activities of Subprocessors are described at:

a. https://cloud.google.com/terms/subprocessors (https://cloud.google.com/terms/third-party-suppliers) for Google Cloud Platform; and

b. https://workspace.google.com/intl/en/terms/subprocessors.html (https://workspace.google.com/intl/en/terms/subprocessors.html) for Google Workspace and Cloud Identity.

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 the processing of Customer Personal Data is subject to European Data Protection Law, the data protection obligations described in this Addendum (as referred to in Article 28(3) of the GDPR, if applicable), are imposed on the Subprocessor; and

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

11.4 *Opportunity to Object to Subprocessor Changes*.

a. When any New Subprocessor is engaged 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 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:

a. at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo) for Google Cloud Platform;

b. at https://support.google.com/a/contact/googlecloud_dpr (https://support.google.com/a/contact/googlecloud_dpr) for Google Workspace and Cloud Identity (while Administrators are signed in to their Admin Account); or

c. as described in the Notices section of the applicable Agreement.

12.2 *Google's Processing Records*. Google will keep appropriate documentation of its processing activities as required by the GDPR. To the extent the GDPR requires Google to collect and maintain records of certain information relating to Customer, Customer will use the Admin Console to supply such information and keep it accurate and up-to-date. Google may make any such information available to the Supervisory Authorities if required by the GDPR.

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. Interpretation

13.1 *Precedence*.

a. To the extent of any conflict or inconsistency between:

i. this Addendum and the remainder of the Agreement, this Addendum will prevail; and

ii. 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.

b. For clarity, if Customer has entered more than one Agreement, this Addendum will amend each of the Agreements separately.

13.2 *Legacy UK SCCs*. The supplementary terms for UK GDPR transfers in the SCCs will, as of 21 September 2022, supersede and terminate any standard contractual clauses approved under the UK GDPR or Data

Protection Act 2018 and previously entered into by Customer and Google.

13.3 *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.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Services and TSS 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 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. 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:

1. tightly controlling the size and make-up of Google's attack surface through preventative measures;
2. employing intelligent detection controls at data entry points; and
3. 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/or 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 and, for Google Workspace and Cloud Identity: (i) Google logically separates each End User's data from the data of other End Users; and (ii) 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). 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.

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) of this Addendum, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Previous versions of Data Processing and Security Terms:

June 30, 2022 (/terms/data-processing-addendum/index-20220630) *September 24, 2021* (/terms/data-processing-terms/index-20210924) *August 19, 2020* (/terms/data-processing-terms/index-20200819)

Digital Millennium Copyright Act

The Digital Millennium Copyright Act

It's Google's policy to respond to clear notices of alleged copyright infringement. Our response to these notices may include removing or disabling access to material claimed to be the subject of infringing activity and/or terminating subscribers. If we take action in response to a notice, we may try to notify the alleged infringer or the operator of the affected site.

We may also document notices of alleged infringement on which we act. We may forward the content in your notice to the nonprofit organization Lumen, which publishes these notices after removing certain personal information. You can see an example of such a publication here. For products like Google Web Search, we provide a link to the notice as published by Lumen in place of the removed content.

This page provides instructions for filing the following types of complaints:

- Infringement Notification
- Counter notification

Infringement Notification

To file a notice of infringement with us, please file a complaint using the steps available at our legal troubleshooter. By selecting the appropriate product, the form will prompt you to provide all the information listed below that is required to submit a valid DMCA complaint. Please note that you will be liable for damages (including costs and attorneys' fees) if you materially misrepresent that a product or activity is infringing your copyrights. Indeed, in a past case (please see http://www.onlinepolicy.org/action/legpolicy/opg_v_diebold/ for more information), a company that sent an infringement notification seeking removal of online materials that were protected by the fair use doctrine was ordered to pay such costs and attorneys fees. The company agreed to pay over $100,000. Accordingly, if you are not sure whether material available online infringes your copyright, we suggest that you first contact an attorney.

Counter notification

The administrator of an affected site or the provider of affected content may make a counter notification pursuant to sections 512(g)(2) and (3) of the Digital Millennium Copyright Act. When we receive a counter notification, we may reinstate the material in question.

Please click on the relevant link below if you would like to file a counter notice for one of the following products:

Blogger
Web Search

If your issue relates to a product not listed above, please find it on our legal troubleshooter and choose the “Counter Notice” option. Please note that you will be liable for damages (including costs and attorneys' fees) if you materially misrepresent that a product or activity is not infringing the copyrights of others. Accordingly, if you are not sure whether certain material infringes the copyrights of others, we suggest that you first contact an attorney.

When filling out our counter notice form, please be sure to identify the specific URLs or other unique identifying information of material that Google has removed or to which Google has disabled access.

Account Termination

Many Google Services do not have account holders or subscribers. For Services that do, Google will, in appropriate circumstances, terminate repeat infringers. If you believe that an account holder or subscriber is a repeat infringer, please follow the instructions above to contact Google and provide information sufficient for us to verify that the account holder or subscriber is a repeat infringer.

Terms and Conditions

Overview of our brand terms and conditions

- If granted permission to use Google Brand Features, you will do so in accordance with our terms.
- If you are using Google Brand Features, you must indicate that those features belong to us.
- Our grant of permission at one point does not prevent us from revoking that permission at a later point.
- You agree that Google owns its brand features and that you will not challenge or attempt to challenge them.
- Google Brand Features are provided “as is.”

Our complete brand terms and conditions

If Google approves your request to use any Google trademarks, logos, web pages, screenshots, or other distinctive features (“Google Brand”), you agree to be bound by the following terms and conditions (the “Agreement”).

You agree to comply with the Guidelines for Third Party Use of Google Brand Features. So long as you do so, and provided that Google expressly approves your permission request, Google grants you a non-transferable, non-exclusive, royalty-free limited license to use the Google’s Brand Features set forth in your corresponding Permission Request Form for the sole purpose and only for the materials set forth therein.

Any use of the Google Brand Features must be accompanied by a notice that clearly indicates that the Google Brand Features are trademarks or distinctive brand features of Google LLC. Google reserves the right in its sole discretion to terminate or modify your permission to display the Google Brand Features and to take action against any use that does not conform to these terms and conditions, infringes any Google intellectual property or other right, or violates applicable law.

Except as set forth above, nothing herein grants or should be deemed to grant to you any right, title or interest in or to the Google Brand Features. Your use of the Google Brand Features will inure to the benefit of Google.

You agree not to challenge or assist others to challenge the Google Brand Features (except to the extent such restriction is prohibited by applicable law), and you agree not to register or attempt to register any domain names, trademarks, trade names, or other distinctive brand features that are confusingly similar to those of Google.

The Google Brand Features are provided “as is” and Google disclaims any warranties either expressed or implied by law regarding the Google Brand Features, including warranties of noninfringement. Furthermore, because you are not being charged for use of the Google Brand Features, in no event shall Google be liable to you for the subject matter of this Agreement under any theory of liability including for any direct, indirect, incidental, special, consequential, punitive, exemplary or other damages arising out of this Agreement or the use of the Google Brand Features. This limitation shall apply even if Google was or should have been aware or advised of the possibility of such damages and notwithstanding any failure of essential purpose of any limited remedy stated herein. Some states do not allow exclusion of implied warranties or limitation of liability for incidental or consequential damages, so the above limitations or exclusions may not apply to you.

You may not assign your rights or delegate your obligations under this Agreement without Google’s prior written consent. This Agreement is not intended to benefit, nor shall it be deemed to give rise to, any rights in any third party. This Agreement will be governed by and construed in accordance with the laws of the State of California, without regard to conflict of law principles. The venue for any dispute or claim arising out of or in connection with this Agreement shall be in Santa Clara County, California. The parties are independent contractors. Neither party shall be deemed to be an employee, agent, partner or legal representative of the other for any purpose and neither shall have any right, power or authority to create any obligation or responsibility on behalf of the other. The waiver by Google of a breach of any provision hereof shall not be taken or held to be a waiver of the provision itself. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, such provision shall be changed and interpreted so as to best accomplish the objectives of the original provision to the fullest extent allowed by law and the remaining provisions of this Agreement shall remain in full force and effect. This Agreement, the Guidelines for Third Party Use of Google Brand Features, and the Permission Request Form, constitute the entire agreement between the parties with respect to the subject matter hereof.

Still can't find what you're looking for? Submit your request via our formal request form.

If you’ve found a website that uses a Google trademark inappropriately, we’d like to hear about it. Report inappropriate use of a Google trademark.

App Engine Service Level Agreement (SLA)

During the Term of the agreement under which Google has agreed to provide Google Cloud Platform to Customer (as applicable, the "Agreement"), the Covered Service will provide a Monthly Uptime Percentage to Customer of at least 99.95% (the "Service Level Objective" or "SLO"). If Google does not meet the SLO, and if Customer meets its obligations under this SLA, Customer will be eligible to receive the Financial Credits described below. This SLA states Customer's sole and exclusive remedy for any failure by Google to meet the SLO. Capitalized terms used in this SLA, but not defined in this SLA, have the meaning set forth in the Agreement. If the Agreement authorizes the resale or supply of Google Cloud Platform under a Google Cloud partner or reseller program, then all references to Customer in this SLA mean Partner or Reseller (as applicable), and any Financial Credit(s) will only apply for impacted Partner or Reseller order(s) under the Agreement.

Definitions.

The following definitions apply to the App Engine SLA:

- "**Covered Service**" means the components of the Service listed at the following URL: https://cloud.google.com/appengine/sla_error_rate, or such other URL as may be provided by Google.
- "**Downtime**" means more than a ten percent Error Rate.
- "**Downtime Period**" means, for a Customer Application, a period of five consecutive minutes of Downtime. Intermittent Downtime for a period of less than five minutes will not be counted towards any Downtime Periods.
- "**Error rate**" for the Service is defined with the Covered Services.
- "**Financial Credit**" means the following:

Monthly Uptime Percentage	Percentage of monthly bill for Covered Service which does not meet SLO that will be credited to future monthly bills of Customer
99.00% – < 99.95%	10%
95.00% – < 99.00%	25%
< 95.00%	50%

- "**Monthly Uptime Percentage**" means total number of minutes in a month, minus the number of minutes of Downtime suffered from all Downtime Periods in a month, divided by the total number of minutes in a month.

Customer Must Request Financial Credit. In order to receive any of the Financial Credits described above, Customer must notify Google technical support within thirty days from the time Customer becomes eligible to receive a Financial Credit. Failure to comply with this requirement will forfeit Customer's right to receive a Financial Credit.

Maximum Financial Credit. The aggregate maximum number of Financial Credits to be issued by Google to Customer for any and all Downtime Periods that occur in a single billing month will not exceed 50% of the amount due by Customer for the use of the Covered Service for the applicable month. Financial Credits will be made in the form of a monetary credit applied to future use of the Service and will be applied within 60 days after the Financial Credit was requested.

SLA Exclusions. The SLA does not apply to any: (a) features designated Alpha or Beta (unless otherwise set forth in the associated Documentation), (b) features excluded from the SLA (in the associated Documentation), or (c) errors: (i) caused by factors outside of Google's reasonable control; (ii) that resulted from Customer's software or hardware or third party software or hardware, or both; (iii) that resulted from abuses or other behaviors that violate the Agreement; or (iv) that resulted from being limited by quotas listed in the Admin Console.

PREVIOUS VERSIONS *(Last modified January 30, 2020)*

Data Catalog Service Level Agreement (SLA)

During the Term of the agreement under which Google has agreed to provide Google Cloud Platform to Customer(as applicable, the "Agreement"), the Covered Service will provide a Monthly Uptime Percentage to Customer(the "Service Level Objective" or "SLO") as follows:

Covered Service	Monthly Uptime Percentage
Data Catalog API usage	>=99.9%

If Google does not meet the SLO, and if Customer meets its obligations under this SLA, Customer will be eligible to receive the Financial Credits described below. Monthly Uptime Percentage and Financial Credit are determined on a calendar month basis per Project per Region. This SLA states Customer's sole and exclusive remedy for any failure by Google to meet the SLO. Capitalized terms used in this SLA, but not defined in this SLA, have the meaning set forth in the Agreement. If the Agreement authorizes the resale or supply of Google Cloud Platform under a Google Cloud partner or reseller program, then all references to Customer in this SLA mean Partner or Reseller (as applicable), and any Financial Credit(s) will only apply for impacted Partner or Reseller order(s) under the Agreement.

Definitions

The following definitions apply to the SLA:

- "**Back-off Requirements**" means, when an error occurs, subsequent repeated calls must be delayed for a period of time according to the following escalation: after the first error, there is a minimum back-off interval of 1 second and for each consecutive error, the back-off interval increases exponentially up to 32 seconds.
- "**Covered Service**" means Data Catalog API usage.
- "**Downtime**" means more than a 5% percent Error Rate and is measured based on server side Error Rate.
- "**Downtime Period**" means a period of five or more consecutive minutes of Downtime. Partial minutes or intermittent Downtime for a period of less than five minutes will not count towards any Downtime Periods.
- "**Error Rate**" means the number of Valid Requests that result in a response with HTTP Status 500 and Code "Internal Error" divided by the total number of Valid Requests during that period, subject to a minimum of 2000 Valid Requests in the measurement period. Repeated identical requests do not count towards the Error Rate unless they conform to the Back-off Requirements.
- "**Financial Credit**" means the following:

Monthly uptime percentage	Percentage of monthly bill for the respective Covered Service in the Region affected that does not meet SLO that will be credited to Customer's future monthly bills
99.0% - < 99.9%	10%
95.0% - < 99.0%	25%
< 95.0%	50%

- "**Monthly Uptime Percentage**" means total number of minutes in a month, minus the number of minutes of Downtime suffered from all Downtime Periods in a month, divided by the total number of minutes in a month.
- "**Region**" means the applicable region identified at https://cloud.google.com/about/locations.
- "**Valid Requests**" are requests that conform to the Documentation, and that would normally result in a non-error response.

Customer Must Request Financial Credit

In order to receive any of the Financial Credits described above, Customer must notify Google technical support within 30 days from the time Customer becomes eligible to receive a Financial Credit. Customer must also provide Google with log files showing Downtime and the date and time it occurred. If Customer does not comply with these requirements, Customer will forfeit its right to receive a Financial Credit.

Maximum Financial Credit

The maximum aggregate number of Financial Credits issued by Google to Customer for all Downtime Periods in a single billing month will not exceed 50% of the amount due from Customer for the Covered Service for the applicable month. Financial Credits will be in the form of a monetary credit applied to future use of the Covered Service and will be applied within 60 days after the Financial Credit was requested.

SLA Exclusions

The SLA does not apply to any (a) features or services designated pre-general availability (unless otherwise set forth in the associated Documentation); (b) features or services excluded from the SLA (in the associated Documentation); or (c) errors (i) caused by factors outside of Google's reasonable control; (ii) that resulted from Customer's software or hardware or third party software or hardware, or both; (iii) that resulted from abuses or other behaviors that violate the Agreement; or (iv) that resulted from quotas applied by the system or listed in the Documentation or Admin Console.

Last modified November 8, 2021