



Google Cloud Terms of Service for G-Cloud 15 - Lot 1a, Lot 2a and Lot 2b

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

- 1.1. General. These terms and conditions ("Agreement") govern the Buyer's use of the Services purchased under Lot 1a, Lot 2a and Lot 2b (as applicable) via the Digital Platform and contracted for under the G-Cloud 15 Framework Agreement and G-Cloud 15 Call-Off Contract.
- 1.2. Use of the Services. Notwithstanding any provision to the contrary in this Agreement, if the Buyer uses a service which does not form part of the Services purchased under a G-Cloud 15 Call-Off Contract, including making a Service Request via the Supplier's Portal ("Out of Scope Services"), the Buyer understands that it will not be able to use the Out of Scope Services under the terms of the G-Cloud 15 Framework Agreement and G-Cloud 15 Call-Off Contract. If the Buyer wishes to use the Out of Scope Services, then where the Out of Scope Services are:
 - 1.2.a. available on the Digital Platform, the Parties will need to agree and enter into a separate G-Cloud 15 Call-Off Contract governed by the G-Cloud 15 Framework Agreement; or
 - 1.2.b. not available on the Digital Platform, the Buyer understands that use of the Out of Scope Services will be outside of the Digital Platform (and this procurement process) and subject to the Supplier's standard terms for the relevant Out of Scope Services. For example, if it is a Google Cloud Platform service, the terms available here: <https://cloud.google.com/terms/> will apply.
- 1.3. Prices. The Framework Prices for the Services are set out on the Digital Platform. If a Buyer selects different pricing and discounts through the functionality of the Services, then the Buyer understands that such activity is outside of the G-Cloud 15 Call-Off Contract terms (and this procurement process).
- 1.4. Conflict of provisions. It is acknowledged that where there is a conflict and/or inconsistency in relation to this Agreement and the other documents comprising the Supplier's relationship with the Buyer under G-Cloud 15, the order of precedence will be as set out in the G-Cloud 15 Call-Off Contract.
- 1.5. Governing Law. It is acknowledged that the Agreement is governed by English law as further set out in clause 39 of the General Terms incorporated into the G-Cloud 15 Call-Off Contract and the Parties submit to the exclusive jurisdiction of the English courts in relation to any dispute (contractual or non-contractual) concerning the Agreement, but either Party

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

- 1.6. Reference Documentation. The (i) Google Cloud Terms of Service, (ii) Google Cloud Acceptable Use Policy, (iii) Generative AI Prohibited Use Policy, (iv) Abuse Monitoring, (v) Google Workspace Technical Support Services Guidelines, (vi) Additional Product Terms, (vii) Service Specific Terms, (viii) SecOps Services Summary, (ix) SecOps Service Specific Terms, (x) Google Workspace Service-Specific Terms, Google Cloud Platform Services: Technical Support Services Guidelines, (xi) Service Specific Terms for Looker (original), (xii) Google Cloud Service Level Agreements (Google Cloud Platform), (xiii) SecOps Service Level Agreements, (xiv) Google Workspace Service Level Agreement, (xv) Google's Looker (original) Service Level Agreement (SLA) for Looker Hosted Deployments, (xvi) Google Cloud Services Technical Support Services Guidelines, (xvii) SecOps Services: Technical Support Services Guidelines, and (xviii) Cloud Data Processing Addendum (Customers) are included in this document for reference only.
- 1.7. Support and Complaints. If a Buyer's End User has a complaint which has not been handled via any of the support channels available as further detailed in this document, that End User should email ps-frameworks@google.com for further assistance.
- 1.8. Licence to Use. The licence that the Supplier gives to the Buyer as referred to in clause 10 of the General Terms incorporated into the G-Cloud 15 Call-Off Contract, shall be a reference to the right to access the Services as referred to in the applicable Supplier Licence Terms in the Order Form and shall not constitute a licence by the Supplier to the Buyer.
- 1.9. Data Definitions. References to Government Data, Buyer Content and Buyer Personal Data (as defined in the G-Cloud 15 Call-Off Contract) are references to Customer Data as set out in this Agreement. The Supplier is a Controller of "Service Data", and the processing of such data is subject to the Google Cloud Privacy Notice at <https://cloud.google.com/terms/cloud-privacy-notice> and, in the context of SecOps Services, is subject to <https://cloud.google.com/terms/secops/privacy-notice> as updated from time to time.
- 1.10. Interpretation. When interpreting this Agreement, references to:
 - 1.10.a. Customer means Buyer (as defined in the G-Cloud 15 Call-Off Contract);



- 1.10.b. Google means Supplier (as defined in the G-Cloud 15 Call-Off Contract);
- 1.10.c. Effective Date means the Start Date (as defined in the G-Cloud 15 Call-Off Contract);
- 1.10.d. Services means the Services (as defined in the G-Cloud 15 Call-Off Contract and covering Lot 1a, Lot 2a and/or Lot 2b services only);
- 1.10.e. Term means the Term (as defined in the G-Cloud 15 Call-Off Contract);
- 1.10.f. Services means Goods (as defined in the G-Cloud 15 Call-Off Contract) (only where usage of the term “Goods” may be relevant to the Services being provided);
- 1.10.g. “Third Party Offerings” (as defined by Google) are excluded from Software, COTS Software and Cloud Products (each as defined in the G-Cloud 15 Call-Off Contract);
- 1.10.h. where specified in the Call-Off Contract, Software (as defined in the G-Cloud 15 Call-Off Contract) means “Premium Software” (as defined in Google’s Service Specific Terms);
- 1.10.i. to the extent applicable to some of the Deliverables (as defined in the G-Cloud 15 Call-Off Contract) under the relevant Order Form and/or Call-Off Contract, the licence that the Supplier gives to the Buyer as referred to in clause 10 of the General Terms and/or Call-Off Schedule 1 incorporated into the G-Cloud 15 Call-Off Contract shall be a reference to Cloud Products (as defined in the G-Cloud 15 Call-Off Contract) licensed under the applicable Supplier Licence Terms in the Order Form;
- 1.10.j. in respect of the Supplier Data Processing Addendum (or Supplier DPA) and in all other respects, for the avoidance of doubt, Services does not include or constitute Software (each as defined in the G-Cloud 15 Call-Off Contract); and
- 1.10.k. where there is an inconsistency between defined terms, such definition applies to the document within which it is contained, and shall not conflict with other definitions that already exist, such that the documents shall sensibly co-exist.



Contents

1. Google Cloud Terms of Service
2. Google Cloud Acceptable Use Policy
3. Generative AI Prohibited Use Policy
4. Abuse Monitoring
5. Google Workspace Technical Support Services Guidelines
6. Additional Product Terms
7. Service Specific Terms (for Google Cloud Platform and SecOps Services)
 - a. General Service Terms
 - b. Service Terms
 - c. Third Party Terms
 - d. Pricing and Billing Terms
 - e. Partner-Specific Terms
 - f. SecOps Service Specific Terms (text from this landing page with the detailed terms set out at item 9 below)
8. SecOps Services Summary
9. SecOps Service Specific Terms
 - a. General Service Terms
 - b. Service Terms
 - c. Partner-Specific Terms
 - d. Google Cloud Platform Terms
10. Google Workspace Service-Specific Terms
11. Service Specific Terms for Looker (original)
12. Google Cloud Service Level Agreements (Google Cloud Platform)



13. SecOps Service Level Agreements
14. Google Workspace Service Level Agreement
15. Google's Looker (original) Service Level Agreement (SLA) for Looker Hosted Deployments
16. Google Cloud Services Technical Support Services Guidelines
 - a. General Support Services Terms
 - b. Standard Support
 - c. Enhanced Support and Partner-led Enhanced Support
 - d. Premium Support, Partner-led Premium Support, and Tech Partner Premium Support
 - e. [Legacy] Silver, Gold and Platinum Support
 - f. [Legacy] Role-Based Support
 - g. [Legacy] Enterprise Support
17. SecOps Services: Technical Support Services Guidelines
18. Cloud Data Processing Addendum (Customers)
 - a. General Terms
 - b. Appendix 1: Subject Matter and Details of Data Processing
 - c. Appendix 2: Security Measures
 - d. Appendix 3: Specific Privacy Laws
 - e. Appendix 4: Specific Products

Google Cloud Terms of Service



New to Google Cloud? A quick overview of Google Cloud's online contracting can be found [here](https://cloud.google.com/terms/overview?hl=en) (<https://cloud.google.com/terms/overview?hl=en>).

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

If you are accessing the Services as a customer of an unaffiliated Google Cloud reseller, these terms will apply to you in relation to your use of the Services (subject to the "Resold Customers" section of the applicable Service Specific Terms). Notwithstanding the applicability of these terms, if you fall under one of the exempt categories described at <https://cloud.google.com/terms/direct-tos-exemptions> for the applicable Services, these terms do not apply to you, unless you and Google agree otherwise in writing. If you become exempt from these terms after the Effective Date, this will not affect any liability arising between the parties prior to the date that you become exempt.

If you signed an offline variant of this Agreement for use of the Google Cloud Platform Services, Google Workspace Services, SecOps Services, or Looker (original) Services under the same Google Cloud Platform Services, Google Workspace, SecOps Services or Looker (original) Services Account, the terms below do not apply to you, and your offline terms govern your use of the applicable Services.

These Google Cloud Terms of Service (together, the "Agreement") are entered into by Google and the entity or person agreeing to these terms ("Customer") and govern Customer's access to and use of the Services. "Google" has the meaning given at <https://cloud.google.com/terms/google-entity>.

This Agreement is effective when Customer clicks to accept or otherwise agrees to it (the "Effective Date"). If you are accepting on behalf of Customer, you represent and warrant that (i) you have full legal authority to bind Customer to this Agreement; (ii) you have read and understand this Agreement; and (iii) you agree, on behalf of Customer, to this Agreement.



1. Provision of the Services.

1.1 Services Use. During the Term, Google will provide the Services in accordance with this Agreement, including the SLAs, and Customer may use the Services, and integrate the GCP Services and Looker (original) Services into any Customer Application that has material value independent of the Services, in accordance with this Agreement. For clarity, Customer may not integrate the Google Workspace Services or SecOps Services into Customer Applications or create or host Customer Applications using the Google Workspace Services or SecOps Services under this Agreement, and Customer may only integrate Looker (original) Services into a Customer Application as provided in the Service Specific Terms.

1.2 Admin Console. If applicable, Customer will have access to the Admin Console, through which Customer may manage its use of the Services.

1.3 Accounts; Verification to Use GWS Services.

(a) *Accounts.* Customer must have an Account to use the Services and is responsible for the information it provides to create the Account, the security of its passwords for the Account (including any keys for Google APIs) and for any use of its Account. Google has no obligation to provide multiple accounts to Customer.

(b) *Verification to use GWS Services.* Customer must verify a Domain Email Address or a Domain Name to use GWS Services. If Customer does not have valid permission to use the Domain Email Address or does not own or control the Domain Name, then Google will have no obligation to provide Customer with GWS Services and may delete the Account without notice.

1.4 Updates.

(a) *To the Services.* Google may make commercially reasonable updates to the Services from time to time.

(b) *To this Agreement.* Subject to subsections (i) and (ii), Google may make updates to this Agreement from time to time. Google will post any update to this Agreement to <https://cloud.google.com/terms/>. This subsection 1.4(b) does not apply to updates to the URL Terms, which are governed by subsection 1.4(c) below.

(i) With respect to GCP Services and their corresponding TSS, unless otherwise noted by Google, material updates to this Agreement will become effective 30 days after they are posted. Notwithstanding the preceding sentence, to the extent any updates apply to new functionality or are required to comply with applicable law, they will be effective immediately. If Customer does not agree to any update to the Agreement regarding GCP or its TSS, Customer may stop using the GCP Services or TSS. Customer may also terminate this Agreement for convenience under Section 8.4 (Termination for Convenience). Customer's continued use of the GCP Services or TSS after a material update will constitute Customer's consent to such update.

(ii) With respect to GWS Services, SecOpS Services, and Looker (original) Services, and their respective corresponding TSS, material updates to this Agreement will only take effect if and when Customer's Order Term renews.

(c) *To the URL Terms.* Google may make commercially reasonable updates to the URL Terms from time to time by posting any such update at the relevant URL Term. Unless otherwise noted by Google, material updates to the URL Terms will become effective 30 days after they are posted. Notwithstanding the preceding sentence, to the extent the updates apply to new functionality or the Cloud Data Processing Addendum, or are required by applicable law, they will be effective immediately.

(d) *To the Cloud Data Processing Addendum.* Without limiting the generality of Section 1.4(c), Google may only update the Cloud Data Processing Addendum where such update is required to comply with applicable law or expressly permitted by the Cloud Data Processing Addendum, or where such update:

- (i) is commercially reasonable;
- (ii) does not result in a material reduction of the security of the Services;
- (iii) does not expand the scope of or remove any restrictions on Google's processing of "Customer Personal Data," as described in the "Compliance with Customer's Instructions" Section of the Cloud Data Processing Addendum; and
- (iv) does not otherwise have a material adverse impact on Customer's rights under the Cloud Data Processing Addendum.

(e) *Discontinuation of Services.* Subject to the last sentence in this Section 1.4(e) (Discontinuation of Services), Google will notify Customer at least 12 months before:

- (i) discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality; or
- (ii) significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Nothing in this Section 1.4(e) (Discontinuation of Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Services) does not apply to pre-general availability Services, offerings, or functionality. For GWS Services, this Section 1.4(e) will only apply to Core Services and will not apply to Other Services.

1.5 *Software.* If Google makes Software available to Customer, including third-party software, Customer's use of any Software is subject to the applicable provisions in the Service Specific Terms.

2. Payment Terms.

2.1 Billing.

(a) Billing Generally.

Google will issue an electronic bill or invoice to Customer for all Fees, including, if applicable, Fees based on Customer's use of the Services during the applicable Fee Accrual Period and any relevant Fees for TSS. If Google reasonably determines based on evidence available to Google that Customer is at risk of non-payment or that Customer's Account is potentially fraudulent, then Google may invoice or charge Customer more frequently. Customer will pay all Fees in the currency stated in the bill or invoice. If Customer pays by credit card, debit card, or other non-invoiced form of payment, Customer will pay all Fees immediately at the end of the Fee Accrual Period or when otherwise charged by Google. If Customer pays by invoice, Customer will pay Google all invoiced amounts by the Payment Due Date. For GCP Services and GWS Services, Customer may change its payment method to any other method that Google may enable, subject to acceptance by Customer of any additional terms applicable to that payment method. Unless required by law, Customer's obligation to pay all Fees is non-cancellable. For GCP Services, GWS Services, and Looker (original) Services, Google's measurement tools will be used to determine Customer's usage of the Services. Google has no obligation to provide multiple bills. Payments made via wire transfer must include the bank information provided by Google.



(b) *Billing Options for GWS Services.* This subsection 2.1(b) applies only to GWS Services. Customer may elect one of the billing options below or any other option offered by Google when Customer places its order for the Services:

(i) *Flexible Plan.* If Customer selects this option, Customer will not be committed to purchase the Services for a pre-defined term, but will pay Fees based on its daily usage of the Services, billed monthly in arrears. Any partial day of Services usage will be rounded up to a full day of Services usage for the purposes of calculating Fees.

(ii) *Annual/Fixed-Term Plan.* If Customer selects this option, Customer will be committed to purchasing the Services for one or more annual terms (as selected by Customer). Google will bill Customer according to the terms associated with Customer's elections on the Order Form.

Google may change its offering of billing options (including by limiting or ceasing to offer any billing option) upon 30 days' notice to Customer and any such change will take effect at the beginning of Customer's next Order Term. Billing options may not be available to all customers.

2.2 Taxes.

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

(b) Customer will provide Google with any applicable tax identification information that Google may require under applicable law to ensure its compliance with applicable tax regulations and authorities in applicable jurisdictions. Customer will be liable to pay (or reimburse Google for) any taxes, interest, penalties, or fines arising out of any mis-declaration by Customer.

2.3 *Payment Disputes & Refunds.* Any payment disputes must be submitted in good faith before the Payment Due Date. If Google, having reviewed the dispute in good faith, determines that certain billing inaccuracies are attributable to Google, Google will not issue a corrected invoice, but will instead issue a credit memo specifying the incorrect amount in the affected invoice. If a disputed invoice has not yet been paid, Google will apply the credit memo amount to a disputed invoice and Customer will be responsible for paying the resulting net balance due on that invoice. Refunds given by Google for billing inaccuracies under this Section will only be in the form of credit for the Services. Nothing in this Agreement obligates Google to extend credit to any party, and Google may revise or revoke any previously-extended credit at any time.

2.4 *Delinquent Payments; Suspension.* Late payments (which, for clarity, do not include amounts subject to a good faith payment dispute submitted before the Payment Due Date), may bear interest at the rate of 1.5% per month (or the highest rate permitted by law, if less) from the Payment Due Date until paid in full. Customer will be responsible for all reasonable expenses (including attorneys' fees) incurred by Google in collecting such delinquent amounts. Further, in the event of any late payment for the Services, Google may Suspend the Services.

2.5 *No Purchase Order Number Required.* Customer is obligated to pay all applicable Fees without any requirement for Google to provide a purchase order number on Google's invoice (or otherwise).

2.6 Price Revisions. Google may change the Prices at any time unless otherwise expressly agreed in an addendum or Order Form. For GWS Services and Looker (original) Services only, (a) Google will notify Customer at least 30 days in advance of any changes, and (b) Customer's pricing will change if and when Customer's Order Term renews after the 30-day period. If Customer objects to any change in Prices, Customer may terminate this Agreement for convenience under Section 8.4 (Termination for Convenience).

3. Customer Obligations.

3.1 Compliance. Customer will (a) ensure that Customer and its End Users' use of the Services complies with this Agreement, (b) use commercially reasonable efforts to prevent and terminate any unauthorized use of, or access to, the Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Services, Account, or Customer's password of which Customer becomes aware. Google reserves the right to investigate any potential violation of the AUP by Customer, which may include reviewing Customer Applications, Customer Data, or Projects.

3.2 Privacy. 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 this Agreement.

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

3.4 Documentation. Google may provide Documentation for Customer's use of the Services.

3.5 Copyright. Google responds to notices of alleged copyright infringement and terminates the Accounts of repeat infringers in appropriate circumstances as required to maintain safe harbor for online service providers under the U.S. Digital Millennium Copyright Act.

3.6 Third-Party Content Enforcement (or GCP Services). If Customer's primary use of the GCP Services is to host third-party content or facilitate the sale of goods or

services between third parties on its platform, Customer will take the following steps to enforce compliance with the AUP: (a) publish policies defining what content is prohibited on its platform (e.g., illegal content); (b) maintain a publicly accessible method (e.g., webform or email alias) to receive notices of violation of that policy (in addition to a monitored communications channel for Google); and (c) promptly review and address any such notices, and remove content where appropriate.

3.7 Additional Terms for GWS Services. The following terms apply only to GWS Services:

(a) *Additional Products and Third-Party Offerings.* Optional Additional Products and Third-Party Offerings may be available for use in conjunction with the Services, and may be enabled or disabled through the Admin Console. Any use of Additional Products is subject to the Additional Product Terms, which are incorporated by reference into the Agreement and which may be updated by Google from time to time. Any use of Third-Party Offerings is subject to separate terms and policies with the relevant service provider.

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

(c) *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 GWS Services abuse.

(d) *Requesting Additional 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.

4. Suspension.

4.1 AUP Violations. If Google becomes aware that Customer's or any End User's use of the Services violates the AUP, Google will notify Customer and request that Customer correct the violation. If Customer fails to correct the violation within 24 hours of Google's request, then Google may Suspend all or part of Customer's use of the Services until the violation is corrected. For GWS Services, Suspension of the Services may include removal or unsharing of content that violates the AUP.

4.2 Other Suspension. Notwithstanding Section 4.1 (AUP Violations), Google may immediately Suspend all or part of Customer's use of the Services if (a) Google reasonably believes Suspension is needed to protect the Services, Google's infrastructure supporting the Services, or any other customer of the Services (or their end users); (b) there is suspected unauthorized third-party access to the Services; (c) Google reasonably believes that immediate Suspension is required to comply with any applicable law; or (d) Customer is in breach of Section 3.3 (Restrictions) or the Service Specific Terms. Google will lift any such Suspension when the circumstances giving rise to the Suspension have been resolved. At Customer's request, Google will, unless prohibited by applicable law, notify Customer of the

basis for the Suspension as soon as is reasonably possible. For Suspension of End User Accounts for GWS Services, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

4.3 Generative AI Safety and Abuse for GCP Services. Google uses automated safety tools to detect abuse of Generative AI Services. Notwithstanding the "Handling of Prompts and Generated Output" section in the Service Specific Terms for GCP Services, if these tools detect potential abuse or violations of Google's AUP (<https://cloud.google.com/terms/aup?hl=en>) or Prohibited Use Policy (<https://policies.google.com/terms/generative-ai/use-policy>), Google may log Customer prompts solely for the purpose of reviewing and determining whether a violation has occurred. See the Abuse Monitoring (<https://docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/abuse-monitoring>) documentation page for more information about how logging prompts impacts Customer's use of the GCP Services.

5. Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features within the GWS Services.

5.1 Intellectual Property Rights. Except as expressly stated in this Agreement, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's 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.

5.2 Protection of Customer Data. Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. Google has implemented and will maintain technical, organizational, and physical measures to protect Customer Data, as further described in the Cloud Data Processing Addendum. If you are accessing the Services as a customer of an unaffiliated Google Cloud reseller, this Section 5.2 (Protection of Customer Data) is subject to the "Resold Customers" section of the applicable Service Specific Terms.

5.3 Customer Feedback. At its option, Customer may provide feedback or 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.

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

6. Technical Support Services.

6.1 By Customer. Customer is responsible for technical support of its Customer Applications and Projects.

6.2 By Google. Subject to payment of applicable support Fees, Google will provide TSS to Customer during the Term in accordance with the TSS Guidelines. Certain TSS levels include a minimum recurring Fee as described at (a) for GCP Services,

SecOps Services, and Looker Services, <https://cloud.google.com/skus>, and (b) for GWS Services, at <https://workspace.google.com/terms/tssg.html>. If Customer downgrades its TSS level during any calendar month, Google may continue to provide TSS at the same level and for the same TSS Fees as applied before the downgrade for the remainder of that month.

7. Confidential Information.

7.1 Obligations. The recipient will only use the disclosing party's Confidential Information to exercise the recipient's rights and fulfill its obligations under this Agreement, and will use reasonable care to protect against the disclosure of the disclosing party's Confidential Information. The recipient may disclose Confidential Information only to its and its Affiliates' employees, agents, subcontractors, or professional advisors ("Delegates") who need to know it and who have agreed in writing (or in the case of professional advisors are otherwise bound) to keep it confidential. The recipient will ensure that its Delegates use the received Confidential Information only to exercise rights and fulfill obligations under this Agreement.

7.2 Required Disclosure. Notwithstanding any provision to the contrary in this Agreement, the recipient or its Affiliate may also disclose Confidential Information to the extent required by applicable Legal Process; provided that the recipient or its Affiliate uses commercially reasonable efforts to (a) promptly notify the other party before any such disclosure of its Confidential Information, and (b) comply with the other party's reasonable requests regarding its efforts to oppose the disclosure. Notwithstanding the foregoing, subsections (a) and (b) above will not apply if the recipient determines that complying with (a) and (b) could (i) result in a violation of Legal Process; (ii) obstruct a governmental investigation; or (iii) lead to death or serious physical harm to an individual.

8. Term and Termination.

8.1 Agreement Term. The term of this Agreement (the "Term") will begin on the Effective Date and continue until this Agreement is terminated as stated in this Section 8 (Term and Termination).

8.2 GWS Services Renewal. The following terms apply only to renewals of GWS Services:

(a) *With a Flexible Plan.* Order Terms for the Flexible Plan are monthly. At the end of each month, the Order Term will automatically renew for another month, unless canceled by Customer via the Admin Console.

(b) *With an Annual/Fixed-Term Plan.* At the end of each Order Term for an Annual/Fixed-Term Plan, the GWS Services will renew consistent with Customer's elections in the Order Form or Admin Console.

(c) *Generally.* Customer may use the Admin Console to adjust the number of End User Accounts to be renewed. Customer will continue to pay Google the then-current Fees for each renewed End User Account unless Customer and Google mutually agree otherwise. If either party does not want the GWS Services to renew, then it must notify the other party to this effect at least 15 days before the end of the then-current Order Term, and this notice of non-renewal will take effect at the end of the then-current Order Term.

8.3 Termination for Breach.

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

(b) *Termination of this Agreement.* To the extent permitted by applicable law, either party may terminate this Agreement immediately on written notice if the other party is in material breach of this Agreement and fails to cure that breach within 30 days after receipt of written notice of the breach.

8.4 Termination for GCP Services Inactivity. Google reserves the right to terminate the provision of GCP Services to a Project upon 30 days' advance notice if, for a period of 60 days (a) Customer has not accessed the Admin Console or the Project has had no network activity and (b) such Project has not incurred any Fees for such Services.

8.5 Termination for Convenience. Customer may stop using the Services at any time. Subject to any financial commitments in an Order Form or addendum to this Agreement, Customer may terminate this Agreement for its convenience at any time on prior written notice and, upon termination, must cease use of the applicable Services. For purposes of GCP Services and TSS only, Google may terminate this Agreement or any applicable Order Form for its convenience at any time with 30 days' prior written notice to Customer. For the avoidance of doubt, any termination of this Agreement by Google for its convenience pursuant to the preceding sentence will not impact any active GWS Services, SecOps Services, or Looker (original) Services Order Forms, and this Agreement will continue to govern such GWS Services, SecOps Services, or Looker (original) Services Order Forms, as applicable, until their expiration or termination pursuant to this Agreement.

8.6 Termination Due to Applicable Law; Violation of Laws. Google may terminate this Agreement immediately on written notice if Google reasonably believes that (a) continued provision of any Service used by Customer would violate applicable law(s) or (b) Customer has violated or caused Google to violate any Anti-Bribery Laws or Export Control Laws.

8.7 Effect of Termination or Non-Renewal. Subject to the last sentence of Section 8.5 (Termination for Convenience), if this Agreement terminates, then all Order Forms also terminate. If this Agreement or an Order Form is terminated or not renewed, then (a) all rights and access to the Services (or in the case of termination of an Order Form, the applicable Services) will terminate (including access to Customer Data, if applicable), unless otherwise described in this Agreement or the Order Form, and (b) all Fees owed by Customer to Google under this Agreement or Order Form, as applicable, are immediately due upon Customer's receipt of the final electronic bill or as stated in the final invoice.

8.8 No Refunds. Unless expressly stated otherwise in this Agreement or required by law, termination or non-renewal under any section of this Agreement (including the Cloud Data Processing Addendum or any Order Form) will not oblige Google to refund any Fees.

9. Publicity. Neither party may use the other party's Brand Features or issue, publish, or present a press release, blog post, speech, social media post, or investor relations call or announcement discussing Customer's use of the Services or this Agreement without the written consent of the other party, except as expressly permitted in this Agreement. Subject to the preceding sentence, Customer may state publicly that it is a Google Cloud customer and display Brand Features in



accordance with the Branding Guidelines. Google may use Customer's name and Brand Features in online or offline promotional materials of the Services. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features.

10. Representations and Warranties. Each party represents and warrants that (a) it has full power and authority to enter into this Agreement, and (b) it will comply with all laws applicable to its provision, receipt, or use of the Services, as applicable.

11. Disclaimer. Except as expressly provided for in this Agreement, Google does not make and expressly disclaims to the fullest extent permitted by applicable law (a) any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, fitness for a particular use, title, noninfringement, or error-free or uninterrupted use of the Services or Software; and (b) any representations about content or information accessible through the Services.

12. Limitation of Liability.

12.1 Limitation on Indirect Liability. To the extent permitted by applicable law and subject to Section 12.3 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to this Agreement for any (a) indirect, consequential, special, incidental, or punitive damages or (b) lost revenues, profits, savings, or goodwill.

12.2 Limitation on Amount of Liability. Each party's total aggregate Liability for damages arising out of or relating to this Agreement in connection with the GCP Services, GWS Services, SecOps Services, or Looker (original) Services, as applicable, is limited to the Fees Customer paid for such Services during the 12 month period before the event giving rise to Liability, except Google's total aggregate Liability for damages arising out of or related to Services or Software provided free of charge is limited to \$5,000.

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

- (a) its fraud or fraudulent misrepresentation;
- (b) its obligations under Section 13 (Indemnification);
- (c) its infringement of the other party's Intellectual Property Rights;
- (d) its payment obligations under this Agreement; or
- (e) matters for which liability cannot be excluded or limited under applicable law.

13. Indemnification.

13.1 Google Indemnification Obligations. Google will defend Customer and its Affiliates using the Services under Customer's Account and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that any Service or any Google Brand Feature, in each case used in accordance with this Agreement, infringes the third party's Intellectual Property Rights.

13.2 Customer Indemnification Obligations. 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 Application, Project, Customer Data, or Customer Brand Features; or (b) Customer's or an End User's use of the Services in breach of the AUP or Section 3.3 (Restrictions).

13.3 Exclusions. Sections 13.1 (Google Indemnification Obligations) and 13.2 (Customer Indemnification Obligations) will not apply to the extent the underlying allegation arises from (a) the indemnified party's breach of this Agreement, (b) a combination of the indemnifying party's technology or Brand Features with materials not provided by the indemnifying party under this Agreement, unless the combination is required by this Agreement, or (c) in the case of Google or any of its Affiliates as the indemnifying party, any Services provided to Customer free of charge.

13.4 Conditions. Sections 13.1 (Google Indemnification Obligations) and 13.2 (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 13.4(a) prejudices the defense of the Third-Party Legal Proceeding, the indemnifying party's obligations under Section 13.1 (Google Indemnification Obligations) or 13.2 (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.

13.5 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 alternative that has materially equivalent functionality.

(b) If Google does not believe the remedies in Section 13.5(a) are commercially reasonable, then Google may Suspend or terminate Customer's use of the impacted Services. If Google terminates the impacted Services, then upon Customer request Google will refund to Customer any unused prepaid Fees that Customer paid to Google for use of the terminated Services.

13.6 Sole Rights and Obligations. Without affecting either party's termination rights and to the extent permitted by applicable law, this Section 13 (Indemnification) states the parties' sole and exclusive remedy under this Agreement for any third-party allegations of Intellectual Property Rights infringement covered by this Section 13 (Indemnification).

14. Miscellaneous.

14.1 Notices. Under this 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.

14.2 *Emails*. The parties may use emails to satisfy written approval and consent requirements under this Agreement.

14.3 *Assignment*. Neither party may assign any part of this Agreement without the written consent of the other, except to an Affiliate where (a) the assignee has agreed in writing to be bound by the terms of this Agreement, and (b) the assigning party has notified the other party of the assignment. Any other attempt to assign is void. If Customer assigns this Agreement to an Affiliate in another jurisdiction such that there is a change in the Google contracting entity as defined at <https://cloud.google.com/terms/google-entity> this Agreement is automatically assigned to the new Google contracting entity.

14.4 *Change of Control*. If a party experiences a change of Control other than as part of an internal restructuring or reorganization (for example, through a stock purchase or sale, merger, or other form of corporate transaction), that party will give written notice to the other party within 30 days after the change of Control.

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

14.6 *Subcontracting*. Google may subcontract obligations under this Agreement but will remain liable to Customer for any subcontracted obligations.

14.7 *No Agency*. This Agreement does not create any agency, partnership, or joint venture between the parties.

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

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

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

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

14.12 *U.S. Governing Law*.

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

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

(c) *For All Other Entities*. If Customer is any entity not identified in Section 14.12(a) (U.S. Governing Law for U.S. City, County, and State Government Entities) or (b)

(U.S. Governing Law for Federal Government Entities), then the following applies: ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SERVICES WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING THAT STATE'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA; THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

14.13 Amendments. Except as stated in Sections 1.4(b) (Updates: To this Agreement); 1.4(c) (Updates: To the URL Terms) or (d) (Updates: To the Cloud Data Processing Addendum), any amendment must be in writing, signed by both parties, and expressly state that it is amending this Agreement.

14.14 Survival. The following Sections will survive expiration or termination of this Agreement: Section 2 (Payment Terms), Section 5 (Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features within the GWS Services), Section 7 (Confidential Information), Section 8.7 (Effect of Termination or Non-Renewal), Section 11 (Disclaimer), Section 12 (Limitation of Liability), Section 13 (Indemnification), and Section 14 (Miscellaneous).

14.15 Entire Agreement. This Agreement sets out all terms agreed between the parties and supersedes all other agreements between the parties relating to its subject matter. In entering into this Agreement, neither party has relied on, and neither party will have any right or remedy based on, any statement, representation, or warranty (whether made negligently or innocently), except those expressly stated in this Agreement. The URL Terms are incorporated by reference into this Agreement. After the Effective Date, Google may provide an updated URL in place of any URL in this Agreement.

14.16 Conflicting Terms. If there is a conflict between the documents that make up this Agreement, the documents will control in the following order (of decreasing precedence): the Cloud Data Processing Addendum, any applicable Order Form, the remainder of this Agreement (excluding the URL Terms), and the URL Terms (excluding the Cloud Data Processing Addendum).

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

14.18 Conflicting Languages. If this Agreement is translated into any language other than English, and there is a discrepancy between the English text and the translated text, the English text will govern unless expressly stated otherwise in the translation. Unless otherwise specified, all references to "\$" in this Agreement refer to United States dollars.

14.19 Definitions.

- "Account" means Customer's Google Cloud Platform, GWS Services, SecOps Services, or Looker (original) Services account, as applicable.
- "Additional Products" means products, services, or applications offered by Google or its Affiliates that are not incorporated into the GWS Services but that may be accessible for use in conjunction with the GWS Services.
- "Additional Product Terms" means, for GWS Services only, the then-current terms stated at https://workspace.google.com/terms/additional_services.

- "Admin Account" means a type of End User Account that Customer (or Reseller, if applicable) may use to administer the GWS Services.
- "Admin Console" means the online console(s) or dashboard provided by Google to Customer for administering the applicable Services.
- "Administrators" mean the Customer-designated personnel who administer the GWS Services to End Users on Customer's behalf, and have the ability to access Customer Data and 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.
- "Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.
- "Anti-Bribery Laws" means all applicable commercial and public anti-bribery laws, including the U.S. Foreign Corrupt Practices Act of 1977 and the UK Bribery Act 2010, that prohibit corrupt offers of anything of value, either directly or indirectly, to anyone, including government officials, to obtain or keep business or to secure any other improper commercial advantage. Government officials include: any government employees, candidates for public office, members of royal families, and employees of government-owned or government-controlled companies, public international organizations, and political parties.
- "AUP" means the then-current acceptable use policy for the Services stated at <https://cloud.google.com/terms/aup>.
- "BAA" or "Business Associate Agreement" is an amendment to this Agreement covering the handling of Protected Health Information (as defined in HIPAA).
- "Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.
- "Branding Guidelines" means Google's then-current Google branding guidelines at https://services.google.com/fh/files/misc/external_customer_co_branding_eligibility.pdf, as may be updated by Google from time to time.
- "Cloud 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-addendum>.
- "Confidential Information" means information that one party (or an Affiliate) discloses to the other party under or in connection with this Agreement, and which is marked as confidential or would normally under the circumstances be considered confidential information. It does not include information that is independently developed by the recipient, is rightfully given to the recipient by a third party without confidentiality obligations, or becomes public through no fault of the recipient. Subject to the preceding sentence, Customer Data is considered Customer's Confidential Information.

- "Control" means control of greater than 50 percent of the voting rights or equity interests of a party.
- "Core Services" means, for GWS Services only, the then-current "Core Services" as described at https://workspace.google.com/intl/en/terms/user_features/, excluding any Third-Party Offerings.
- "Customer Application" means a software program that Customer creates or hosts using the GCP Services or Looker (original) Services, as applicable.
- "Customer Data" means (a) for GCP Services, Looker (original) Services, and SecOps Services, 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; and (b) for GWS Services, data submitted, stored, sent or received via the Services by Customer or its End Users.
- "Documentation" means the Google documentation (as may be updated from time to time) in the form generally made available by Google to its customers for use with the Services, including at <https://cloud.google.com/docs/> and any Looker (original) user guides and manuals Google provides Customer for its internal use.
- "Domain Email Address" means the email address on the Domain Name for use in connection with the GWS Services.
- "Domain Name" means the domain name specified in the Order Form to be used in connection with the GWS Services.
- "End Users" means the individuals who are permitted by Customer 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 GWS Services in order for an End User to use the GWS Services.
- "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.
- "Fee Accrual Period" means (a) a calendar month or other period or billing frequency (b) for GCP Services only, a period in which Customer reaches a designated spend threshold, in each case specified by Google in the Admin Console or in an Order Form.
- "Fees" means the applicable fees for each Service, Software, TSS, and Third-Party Offerings, plus any applicable Taxes. The Fees for each GCP Service are stated at <https://cloud.google.com/skus/> (incorporated into this Agreement by this reference).
- "GCP Services" or "Google Cloud Platform Services" means the then-current services described at <https://cloud.google.com/terms/services>.

- "Google API" means any application programming interface provided by Google as part of the Services.
- "GWS Services" or "Google Workspace Services" means the then-current Core Services and Other Services. For the avoidance of doubt, GWS Services do not include Google Workspace for Education, which is not governed by this Agreement.
- "High Risk Activities" means activities where the use or failure of the Services would reasonably be expected to lead to death, personal injury, or environmental or property damage (such as the creation or operation of nuclear facilities, air traffic control, life support systems, or 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 (i) settlement amounts approved by the indemnifying party, and (ii) damages and costs finally awarded against the indemnified party by a court of competent jurisdiction.
- "Intellectual Property Rights" means current and future worldwide rights under patent, copyright, trade secret, trademark, and moral rights laws, and other similar rights.
- "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.
- "Looker (original) Services" means the integrated business intelligence and embedded analytics platform (including the software components that connect to APIs) provided as either a deployment hosted by Google or a deployment hosted by Customer, as specified in the applicable Order Form. For clarity, Looker Studio and Looker (Google Cloud core) are GCP Services and are not Looker (original) Services.
- "Notification Email Address" means the email address(es) designated by Customer in the Admin Console, or if none exists, the applicable Order Form.
- "Order Form" means (a) an order form, statement of work, or other ordering document issued by Google under this Agreement and executed by Customer and Google; or (b) an order placed by Customer via a Google website or the Services, in each case specifying the Services Google will provide to Customer.
- "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 this Agreement.
- "Other Services" means, for GWS Services only, the then-current "Other Services" as described at https://workspace.google.com/intl/en/terms/user_features/, excluding any Third-Party Offerings.

- "Payment Due Date" means the payment due date set out in the applicable Order Form, or if not specified, 30 days from the invoice date.
- "Project" means, as applicable:
 - (i) a collection of Google Cloud Platform resources configured by Customer via the GCP Services; or
 - (ii) an instance of the SecOps Services configured and used by Customer.
- "SecOps Services" means the then-current services described at <https://cloud.google.com/terms/secops/services>.
- "Service Specific Terms" means, as applicable:
 - (i) For GCP Services, the then-current terms specific to one or more Services stated at cloud.google.com/terms/service-terms;
 - (ii) For GWS Services, the then-current terms specific to one or more services stated at <https://workspace.google.com/terms/service-terms/>;
 - (iii) For SecOps Services, the then-current terms specific to one or more Services stated at <https://cloud.google.com/terms/secops/service-terms>; and
 - (iv) For Looker (original) Services, the then-current terms specific to one or more Services stated at <https://cloud.google.com/terms/looker/legal/customers/service-terms>.
- "Services" means the GCP Services, GWS Services, SecOps Services, or Looker (original) Services, as applicable. In each case, Services exclude any Third-Party Offerings.
- "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.
- "SLA" means, as applicable:
 - (i) For GCP Services, each of the then-current service level agreements at <https://cloud.google.com/terms/sla>;
 - (ii) For GWS Services, the then-current service level agreement at <https://workspace.google.com/terms/sla/>;
 - (iii) For SecOps Services, each of the then-current service level agreements at <https://cloud.google.com/terms/secops/sla>; and
 - (iv) For Looker (original) Services, each of the then-current service level agreements at <https://cloud.google.com/terms/looker/legal/customers/sla>.
- "Software" means any downloadable tools, software development kits, or other such computer software provided by Google in connection with the applicable Services, and any updates Google may make to such Software from time to time, excluding any Third-Party Offerings.
- "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.
- "Term" has the meaning stated in Section 8.1 (Agreement Term) of this Agreement.



- "Third-Party Offerings" means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software, (b) offerings identified in the "Third-Party Terms" section of the applicable Service Specific Terms, and (c) third-party operating systems.
- "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).
- "TSS" means the then-current technical support service provided by Google to Customer under the TSS Guidelines.
- "TSS Guidelines" means Google's technical support services guidelines then in effect for the Services. TSS Guidelines are available at, as applicable:
 - (i) For GCP Services, SecOps Services, and Looker (original) Services, <https://cloud.google.com/terms/tssg/>; and
 - (ii) For GWS Services, <https://workspace.google.com/terms/tssg.html>.
- "URL Terms" means, collectively, the AUP, Cloud Data Processing Addendum, Service Specific Terms, SLA, and TSS Guidelines.

15. Regional Modifications. Customer agrees that the modifications described at <https://cloud.google.com/terms/regional-modifications>, or a successor URL, as may be updated from time to time, apply to the Agreement if Customer's billing address is in the applicable region and will govern to the extent of any conflict with the remainder of the Agreement.

Previous versions of SecOps Services Agreement

May 23, 2024 April 4, 2024 February 14, 2024 December 13, 2023 June 15, 2023
April 3, 2023 February 6, 2023 August 31, 2022 September 20, 2021 October 1, 2020

Previous versions of the VirusTotal Terms of Service

January 27, 2021 December 11, 2018

Previous versions of Looker (original) Services Terms of Service

January 30, 2025 October 16, 2024 December 13, 2023 October 4, 2023
December 7, 2022 February 14, 2022 August 19, 2021 April 1, 2021 November 2, 2020
June 1, 2020 April 30, 2019 April 30, 2019 February 28, 2019

Previous versions of Google Cloud Terms of Service (*Last modified October 13, 2025*)

July 1, 2025 April 22, 2025 January 30, 2025 October 17, 2024 September 30, 2024
November 16, 2023 July 12, 2023 April 19, 2023 February 6, 2023 November 7, 2022
September 20, 2022 March 29, 2022 September 20, 2021 April 1, 2021 November 2, 2020
October 6, 2020 August 31, 2020 August 13, 2020 March 26, 2020 November 21, 2019
July 22, 2019 November 2, 2018 November 1, 2018 October 1, 2018 June 27, 2018
June 15, 2018 June 5, 2018 May 23, 2018 May 18, 2018 April 30, 2018
April 4, 2018 February 8, 2018 January 9, 2018 October 19, 2017





Google Cloud Acceptable Use Policy

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

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

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

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

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



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

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

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

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

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

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

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



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



Generative AI Prohibited Use Policy

Last Modified: December 17, 2024

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

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



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

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

Abuse monitoring

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

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

What's next



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



Google Workspace Technical Support Services Guidelines

Last modified: 8 November 2023

The following technical support services guidelines ('**Guidelines**') apply to support services for Google Workspace Services ('**Services**'), Pre-GA Offerings (and similar offerings) and Chrome, subject to Section 5 (Excluded Services and Editions) below, which identifies the services, editions and offerings that are not eligible for support services. Capitalised terms not defined herein have the meaning set forth in the agreement that governs Customer's use of Google Workspace Services ('**Agreement**').

1. Support Request submission

1.1 **Customer efforts to fix errors.** Prior to making a Request to Google, the Customer will use reasonable efforts to resolve issues and fix any error, bug, malfunction or network connectivity defect without escalation to Google. The Customer Contact may then submit a Request for technical support as specified at <https://support.google.com/a/answer/1047213> or as such URL may be updated by Google.

1.2 **Characterisation of Requests.** The Customer will designate priority when submitting Requests. On receipt of a Request from a Customer Contact, Google will determine whether the Request is a 'Service Unusable', 'Standard Request' or a 'Feature Request' (as defined in section 7 (Definitions)). Any such determination made by Google is final and binding on Customer. Google reserves the right to reclassify Customer's Priority designation if (i) Google believes that Customer's Priority designation is incorrect or (ii) Customer fails to maintain continuous availability, as described in Section 1.3 (Procedures for Acknowledgement and Resolution of Requests). Google will inform the Customer of any such reclassification in Google's response to the support Request. The Customer may appeal any such reclassification to Google's Support management for review through any available support channel. Any reclassifications by Google of the Priority designation pursuant to subsection (ii) will be reversed if Customer resumes continuous availability in accordance with Section 1.3 (Procedures for Acknowledgement and Resolution of Requests).

1.3 **Procedures for Acknowledgement and Resolution of Requests.** When making a Request, the Customer will provide requested diagnostic information including but not limited to: (i) describing the problem, the configuration and the Customer's network; (ii) providing relevant data and (iii) answering questions and assisting Google Support Personnel as appropriate. The Customer must provide up-to-date contact information (i.e. phone number or email address) to assist with data gathering, testing and applying resolutions. In the case of P1 Requests, the Customer must maintain continuous availability until resolution of such Requests.

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

1.5 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 accommodate any such Feature Request in any future update or release.

2. Accessing Support

2.1 Google Help Centre. The Customer's End Users of the Services may access the Google Help Centre at <https://support.google.com/a/> or such other URL as Google may provide. The Customer is responsible for responding to any questions and complaints from End Users or other third parties relating to the Customer's or its End Users' use of the Services, with such support services to be provided at the Customer's own expense.

2.2 Customer PIN. The Customer is required to provide a current Customer PIN when making a Request. The Customer will obtain such Customer PIN in the Admin console in order to access and receive support for the Services from Google. If the Customer is unable to provide the current Customer PIN when prompted, the Customer will only be able to access the Google Help Centre and post a question to its online help forum, until such time as the Customer PIN is restored. The customer PIN may be updated periodically and is only available in the Admin console.

2.3 Compliance with applicable law. Google will not provide TSS if prohibited from doing so by applicable law.

2.4 Pre-General Availability Offerings.

i. **Pre-GA Offerings.** Google has no obligation to provide TSS for Pre-GA Offerings (as defined in the Service Specific Terms) or any offerings identified as 'Preview', 'Alpha', 'Beta', 'Experimental' or similar designation.

ii. **Pre-GA Support Offerings Terms.** Google may make available to Customer pre-general availability technical support services or features, in each case that are identified as 'Preview', 'Alpha', 'Beta', 'Experimental' or similar designation in related documentation or materials or are not yet listed in these Guidelines (collectively, 'Pre-GA Support Offerings'). While Pre-GA Support Offerings are not TSS, Customer's use of Pre-GA Support Offerings is subject to the terms of these Guidelines, as amended by this Section (Pre-GA Support Offerings Terms) and any additional terms provided to Customer in the Google Support Tool or order form or otherwise presented by Google (the 'Additional Pre-GA Support Terms'). In the event of conflict between the terms of these Guidelines and the Additional Pre-GA Support Terms, the Additional Pre-GA Support Terms govern.

a. Pre-GA Support Offerings may be changed, suspended, or discontinued at any time without prior notice to the Customer.

b. At its option, Customer may provide feedback and suggestions about the Pre-GA Support Offerings to Google ('Pre-GA Support Feedback'). If Customer provides Pre-GA Support Feedback, then Google and its Affiliates may use that Pre-GA Support Feedback without restriction and without obligation to



Customer, excluding any Pre-GA Support Feedback marked as Customer Confidential Information.

c. Target initial response times and language support as described in these Guidelines may be different or unavailable for Pre-GA Support Offerings.

3. Chrome Support

3.1 **Availability of Support**. In addition to Requests related to the Services, Google will respond in accordance with these guidelines to Requests related to Chrome:

- i. For all Workspace End-User Accounts;
- ii. If the Customer is paying for 100 or more concurrent Workspace End-User Accounts, for all other end users associated with the Customer's domain.

3.2 **Supported Issue Types**. Google Support Personnel will respond to Requests related to Chrome installation, Chrome Core Functionality, Chrome's security, administrative policies and Chrome's interoperability with Services on Supported Platforms as set forth in these Guidelines. Google may choose to not 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, or device driver or printer problems. If Google makes a code change to resolve a technical issue, the code change is released in an upcoming release and will not be ported back to an earlier version of Chrome.

4. Support Levels

4.1 **Generally**. As part of the customer's order of the services, Google will provide Standard Support to the customer. The Customer may order additional TSS for an additional fee.

4.2 **Standard Support**. Customer will receive the following:

- i. Automatic product upgrades of the Services
- ii. Maintenance updates of the Services
- iii. Online self-help and training for End Users and Administrators designed to assist Customer with implementation and use of the Services
- iv. Ability to submit a support Request
- v. Status Dashboard and support portal providing real-time publicly available status information for the Services

4.3 **Fee Commitments**. Some TSS require a one-year fee commitment. When the Customer enrolls in such TSS, any applicable fees will be pro-rated for that month and then continue to apply for each month in the one-year commitment period.

4.4 **Support Hours and Target Initial Response Times**.

- i. Google will provide access to Google Help Centre support for the Customer on a 24x7 basis.
- ii. Target initial response times.

Target Initial Response Times during the Hours of Operation

Priority	Standard Support	Enhanced Support	Premium Support
P1	4 hours 24x7	1 hour 24x7	15 minutes 24x7

P2	8 hours	4 hours 24x7	2 hours 24x7
P3	24 hours	8 hours	4 hours 24x7
P4	24 hours	8 hours	8 hours

4.5 Enhanced Support. Enhanced Support will be provided in English language (24x7) and in Japanese language during Business Hours. For any Requests in Japanese language submitted outside of Opening Hours, Google will respond within the target initial response times stated for Workspace Standard Support.

i. **Value Add Services.** The Customer may purchase the following Value Add Services for Enhanced Support for an additional fee.

a. **Technical Account Advisor Service (TAAS).** The 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 optimisation of the Services.

4.6 Premium Support.

i. Premium Support will be provided in English language (24x7) and in Japanese language during Business Hours. For any Requests in Japanese language submitted outside of Opening Hours, Google will respond within the target initial response times stated for Workspace Standard Support.

ii. As part of the Premium Support offering, customers 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.

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

a. **Assured Support.** Google will provide TSS for Assured Controls ('Assured Support') in accordance with the Customer-selected support portal controls. All requests for Assured support by the customer must be submitted via the 'new case' option from within the support portal. Notwithstanding Section 6.2 (Language), Google will provide Assured Support in English language only.

4.7 Legacy Standard Support. Notwithstanding any other term of Section 4 (Support levels), the following terms will apply if the Customer enrolled in Standard Support prior to 6 October 2020: P1 Priority Support Requests are responded to with a target initial response time of one hour and are responded to 24x7; and P2, P3 and P4 Priority Support Requests are responded to with an initial target response time of one working day or less.

5. Excluded services and editions

Notwithstanding any term of the Agreement that may indicate otherwise, and in addition to the exclusion set out in Section 2.4(i) (Pre-GA Offerings): (i) Google does not offer TSS for any of the following: Chrome Sync (when included in any edition of Google Workspace for Education); the Google Workspace Essentials Starter edition;

or any Additional Products; and (ii) TSS is provided for AppSheet under the AppSheet support service guidelines at <https://www.appsheet.com/Home/TSSG> and not these Guidelines.

6. General Provisions

6.1 Maintenance. To ensure optimal performance of the Services, Google performs periodic Maintenance. In most cases, Maintenance shall 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 shall 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 shall use commercially reasonable efforts to provide advance notice of such maintenance. Maintenance notices will be provided via the Google Workspace Dashboard, Admin console and/or support portal. In addition, if the Customer subscribes to Maintenance notices, the Customer may also be able to receive email and/or RSS feed notifications of Maintenance.

6.2 Language. Except as stated otherwise in these Guidelines, all support provided by Google Support Personnel pursuant to these Guidelines will be provided in the English language, or during listed hours in one of the additional languages documented in these Guidelines or at <https://support.google.com/a/table/3247295> or such other URL as Google may provide. Support outside of these hours can be obtained via English language support channels.

6.3 Term of Support. Google shall only provide the support services described in these Guidelines during the term of the Agreement and shall have no obligation to provide any support services to the Customer after the expiry or termination of such Agreement.

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

7. Definitions

For the purpose of these Guidelines, the capitalised terms below will have the following meanings:

7.1 'Business Hours' means business hours in Japan, namely, 09:00 to 17:00 on Monday to Friday Japan Standard Time.

7.2 '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 MSI installer provided at the URL <https://www.google.com/chrome/business/> or at another URL that Google may provide.

7.3 'Chrome Core Functionality' means the features and functionality in the latest released Chrome browser version, excluding Google Chrome extensions, Google Play and Google Cloud Print.

7.4 **'Customer Contacts'** means Administrators designated in the Admin Console.

7.5 **'Feature Request'** means a Request by a Customer 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.

7.6 **'Google Support Personnel'** means the Google representatives responsible for handling technical support requests.

7.7 **'Hours of Operation'** means the hours listed at <https://support.google.com/a/table/3247295> for each country except for holidays in local time for each region as documented in the Admin Console.

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

7.9 **'Priority'** means the level of impact that a Request is having on the Customer's operations and is used to establish target response times. Definitions of available priority levels can be found on our Help Centre:

<https://support.google.com/a/answer/1047213>

7.10 **'Request'** means a request from the Customer to Google Support Personnel for technical support to resolve a question or problem regarding the Services and Chrome.

7.11 **'Service Unusable'** means a production issue that prevents more than one of the Customer's End Users from access to, or use of, the Services, or where the Customer's network is not receiving any inbound email (and/or sending outbound email) from the Services. The Customer must identify a Request as Service Unusable by designating it as a P1 Priority support Request.

7.12 **'Standard Request'** means a Request made by Customer to Google that is not a Service Unusable Request or Feature Request.

7.13 **'Supported Platform'** as listed at <https://support.google.com/a/bin/answer.py?answer=2763059> means an operating system and version for which (i) Chrome is released by Google and (ii) support under these Guidelines is provided. 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.

7.14 **'Value Add Services'** means additional TSS available to the Customer for an additional fee.

Previous Versions

Last modified 8 November 2023

8 November 2023

31 May 2023

30 March 2023

14 November 2022

28 April 2022



Additional Product Terms

From time to time, Google may make available one or more Google product(s) and/or service(s) referred to as 'Additional Products' or 'Additional Services' in Customer's Google Workspace Agreement, Cloud Identity Agreement or Hire Agreement (as applicable, the "**Agreement**"). For the purposes of these Additional Product Terms, such product(s) and/or service(s) will be collectively referred to as "**Additional Products**".

If Customer or any End User uses any Additional Products (a) Customer agrees to these Additional Product Terms, which will be incorporated into the applicable Agreement and (b) the separate terms of service applicable to such products will apply to their use of such products as described below. For clarity, such terms of service will each form a separate agreement and are not governed by, or incorporated into, the applicable Agreement.

If Customer does not wish to enable any Additional Products, or if you are acting on behalf of Customer but do not have the requisite authority to bind Customer to these Additional Product Terms, please disable such Additional Products via the functionality of the Services.

1. **Definitions.** All capitalized terms used in these Additional Product Terms have the meanings given to them in the applicable Agreement, unless otherwise defined or stated herein.

2. **Applicable Terms of Service.** The Additional Products will be governed by (a) these Additional Product Terms, and (b) the Google Terms of Service located at <https://policies.google.com/terms> or any other terms of service Google may make available (as applicable, the "**Terms of Service**"). Customer will be responsible under these Additional Product Terms for any failure by its End Users to comply with such Terms of Service. Further details of the Additional Products and Terms of Service are provided at <https://www.google.com/support/a/bin/answer.py?answer=181865> and/or will be otherwise made available by Google. The Additional Products and Terms of Service may be updated or modified by Google from time to time.

3. **Availability.** Additional Products may not be available in all countries.

4. **Technical Support.** Customer is responsible for responding to questions from End Users relating to Customer's or End Users' use of the Additional Products. Google only provides technical support services for the Additional Products to the extent described in the applicable Terms of Service, and will not provide other technical support for the Additional Products unless Google agrees otherwise in writing.

5. **Compliance with Laws.** Customer agrees that it will provide Additional Products to its End Users in compliance with all applicable laws and regulations, including privacy and data protection laws, the US Family Educational Rights and Privacy

Act (FERPA) of 1974, the US Children's Internet Protection Act (CIPA), and the US Children's Online Privacy Protection Act (COPPA) of 1998.

6. Customer Access to End User Data. Customer may be able to access, monitor, delete, rectify, export, use or disclose data provided by and related to End Users in the context of Additional Products or to disable End User Accounts for Additional Products. To the extent Customer has any such abilities, Customer will provide End Users with relevant information and facilitate the exercise of any related rights of End Users under privacy or data protection laws. If Google receives any request from an End User pertaining to Customer's processing of his/her personal data in relation to any Additional Products, Google will advise the End User to submit his/her request to Customer, and Customer will be responsible for responding to the request.

7. End User Consent. Except in relation to End Users described in Section 8 (Parental Consent), Customer will, before it allows any End Users to access or use any Additional Products, obtain and maintain consents from those End Users to the collection and use of their personal information in connection with those Additional Products.

8. Parental Consent. Before Customer allows any End Users who are under the age of 16 (or such other minimum age as is specified in the relevant European Economic Area member state, the UK or Switzerland) and resident in the European Economic Area, the UK or Switzerland, or any other End Users under the age of 18, to access or use any Additional Products, Customer will obtain parental consent for the collection and use of personal data in connection with those Additional Products.

9. Product-Specific Terms.

a. **Google Pay.** A Google Pay account opened by an End User is the End User's personal account and is subject to extensive regulatory requirements and prohibitions. While Customer may suspend an End User's access to his/her Google Pay account, Customer may not use an End User's Google Pay account or make any changes to the information in such Google Pay account. Customer may access information in an End User's Google Pay account only in accordance with Google Pay privacy policies and Customer's privacy policy.

b. **Gemini app.** If Customer or any End User uses Gemini app as an Additional Product: (a) Customer or the End User will have a limited ability to update, manage, export and delete data, as described at https://support.google.com/gemini?p=workspace_edu; and (b) notwithstanding anything to the contrary at https://support.google.com/gemini?p=workspace_edu, Google will not use data or content submitted by



Customer or the End User with an edition of Google Workspace for Education Fundamentals via Gemini app to train or fine-tune Google's generative artificial intelligence models supporting Gemini app unless this processing is explicitly agreed to by the Customer in writing.

10. Refund for Paid Services. If Customer disables an Additional Product for which Customer or an End User has provided payment, Google will not be obliged to refund any fees paid by Customer and/or the End User for unused paid services. Customer will indemnify Google from and against all liabilities, damages, losses, expenses and costs (including settlement costs and reasonable legal fees) arising out of End User claims concerning refunds for such paid services.

11. Severability. If any part of these Additional Product Terms is found to be unenforceable, the remainder of the Additional Product Terms will remain in full force and effect.

12. Modifications. Google may modify these Additional Product Terms from time to time.

13. Interpretation of Conflicting Terms. To the extent of any conflict or inconsistency between these Additional Product Terms and the remainder of the applicable Agreement, the remainder of the Agreement will prevail.



Service Specific Terms

For translations of these Service Specific Terms into other languages, please click on the appropriate link: Bahasa Indonesia

(https://docs.google.com/document/d/1A5r6qGtLbkc3iX7gNQet3i2vpCVmHkdQrP8P54_tU10/edit?tab=t.0) , Deutsch

(<https://services.google.com/fh/files/misc/de-cloud-service-specific-terms.pdf>), Español (Latinoamérica)

(<https://services.google.com/fh/files/misc/es-419-cloud-service-specific-terms.pdf>), Français

(<https://services.google.com/fh/files/misc/fr-cloud-service-specific-terms.pdf>), Italiano

(<https://services.google.com/fh/files/misc/it-cloud-service-specific-terms.pdf>), Nederlands

(<https://services.google.com/fh/files/misc/nl-cloud-service-specific-terms.pdf>), Português

(<https://services.google.com/fh/files/misc/pt-br-cloud-service-specific-terms.pdf>), 한국어

(<https://services.google.com/fh/files/misc/ko-cloud-service-specific-terms.pdf>), 日本語

(<https://services.google.com/fh/files/misc/ja-cloud-service-specific-terms.pdf>)

These Service Specific Terms are incorporated into the agreement under which Google has agreed to provide Google Cloud Platform and SecOps Services (as described at <https://cloud.google.com/terms/services>) to Customer (the “Agreement”). If the Agreement authorizes you to resell or supply Google Cloud Platform under a Google Cloud partner or reseller program, then except for in the section entitled “Partner-Specific Terms”, all references to Customer in the Service Specific Terms refer to you (“Partner” or “Reseller”, as used in the Agreement), and all references to Customer Data in the Service Specific Terms mean Partner Data. If you are accessing the Services as a customer of an unaffiliated Google Cloud reseller, then Section 14 (Resold Customers) of the General Service Terms applies to you. Capitalized terms used but not defined in the Service Specific Terms have the meaning given to them in the Agreement.

General Service Terms

General Definitions.

“*Cloud Data Processing Addendum*” (formerly referred to as the Data Processing and Security Terms) has the meaning given in the Agreement or, if no such meaning is given, means the then-current terms describing data processing and security obligations with respect to Customer Data at

<https://cloud.google.com/terms/data-processing-addendum>.

“*Documentation*” means the then-current Services and / or Software documentation at <https://cloud.google.com/docs/>.

“*Fees URL*” means <https://cloud.google.com/skus>.

“*Scope of Use*” means any limits on installation or usage of Services or Software described at the Fees URL, Admin Console, Documentation, order form, or otherwise presented by Google.

1. Data Location.

a. Additional Definitions.

“Cloud Locations Page” means <https://cloud.google.com/about/locations/>.

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

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

b. Applicable Terms. For any Service listed at

<https://cloud.google.com/terms/data-residency>, Customer may select a specific Region or Multi-Region as detailed in the Cloud Locations Page, and Google will store Customer Data for that Service at rest only within the selected Region or Multi-Region. Google may replicate that Customer Data within any other Region located within the country of the selected Region or within the country or countries of the selected Multi-Region (as applicable) for backup, reliability, debugging, support, maintenance, or security purposes. The Services do not limit the locations from which Customer or Customer End Users may access Customer Data or to which they may move Customer Data. For clarity, Customer Data does not include resource identifiers, attributes, or other data labels. Additional terms regarding configuration of specific Services are in the following sections under “Service Terms”:

(i) AI/ML Data Location; and

(ii) Assured Workloads Data Location.

Services that do not store Customer Data at-rest or process Customer Data in use are also listed on <https://cloud.google.com/terms/data-residency>.

2. Operations of Communications Services. Notwithstanding any telecommunications restrictions in the Agreement, Customer may use the Services for hosting capacity in connection with Customer’s provision of telecommunications services if (a) Customer obtains, maintains, and complies with all necessary regulatory licenses, registrations or other applicable requirements relating to such telecommunications services, and (b) Customer does not use or resell the Services to provide telecommunications connectivity, including for virtual private network services, network transport, or voice or data transmission.

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

a. *License.* Google grants Customer a royalty-free (unless otherwise stated by Google), non-exclusive, non-sublicensable, non-transferable license during the Term to reproduce and use the Software ordered by Customer on systems owned, operated, or managed by or on behalf of Customer in accordance with (i) the Agreement, and (ii) if applicable, the Scope of Use. Customer may authorize its and its Affiliates’ employees, agents, and subcontractors (collectively, “Software Users”) to use the Software in accordance with this subsection. Customer may make a reasonable number of copies of the Software for back-up and archival purposes. For clarity, Software does not constitute Services.

b. *Compliance With Scope of Use.* Within 30 days of Google’s reasonable written request, Customer will provide a detailed written report describing its usage in accordance with the applicable Scope of Use of each Software product used by Customer and its Software Users during the requested period. If requested,

Customer will provide reasonable assistance and access to information to verify the accuracy of Customer's Software usage report(s).

c. *Other Warranties and Compliance.* Each party represents and warrants that it will comply with all laws applicable to its provision or use of the Software. Customer will: (i) ensure that Customer and its Software Users' use of the Software complies with the Agreement (including the Scope of Use) and the restrictions in the Agreement applying to Customer's use of the Services; (ii) use commercially reasonable efforts to prevent and terminate any unauthorized access to or use of the Software; and (iii) promptly notify Google of any unauthorized access to or use of the Software of which Customer becomes aware.

d. *Open Source or Third Party Terms.* If the Software contains open source or third-party components, those components may be subject to separate license agreements, which Google will make available to Customer. Customer is solely responsible for complying with the terms of any third parties from which Customer elects to migrate its workloads onto the Services, and represents and warrants that such third-party sources permit the use of Software to migrate applications away from such sources.

e. *Termination.* On termination or expiration of the Agreement, Customer will stop using all Software and delete all copies.

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

a. *Introduction.* Google makes certain Software available under the Agreement described as "Premium Software" at <https://cloud.google.com/terms/services> ("Premium Software"). Customer will pay applicable Fees for any Premium Software it obtains as described at the Fees URL. Premium Software is Google's Confidential Information.

b. Software Warranty.

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

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

c. *Software Indemnification.* Google's Intellectual Property Rights infringement indemnity obligations under the Agreement apply to Premium Software, and Customer's indemnity obligations under the Agreement with respect to Customer's use of the Services apply to Customer's use of Premium Software. In addition to any other indemnity exclusions in the Agreement, Google's indemnity obligations will not

apply to the extent the underlying allegation arises from modifications to Premium Software not made by Google or use of versions of Premium Software that are no longer supported by Google.

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

e. *Compliance*. Premium Software may transmit to Google metering information reasonably necessary to verify that use of the Premium Software complies with the Scope of Use. Customer will not disable or interfere with the transmission of such metering information.

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

5. Pre-GA Offerings Terms.

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

b. ***Disclaimer***. PRE-GA OFFERINGS ARE PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS OF ANY KIND. Pre-GA Offerings (i) may be changed, suspended or discontinued at any time without prior notice to Customer and (ii) are not covered by any SLA or Google indemnity. Except as otherwise expressly indicated in a written notice or Google documentation, (A) Pre-GA Offerings are not covered by TSS, and (B) the Data Location Section above will not apply to Pre-GA Offerings.

c. ***Liability***. Notwithstanding anything to the contrary in any other limitation of liability Section in the Agreement, with respect to Pre-GA Offerings, Google will not be liable for any amounts in excess of the lesser of (i) the limitation on the amount of liability stated in the Agreement or (ii) \$25,000. Nothing in the preceding sentence will affect any exclusions from any limitation of liability in the Agreement with respect to the following: (A) death or personal injury resulting from negligence, (B) fraud or fraudulent misrepresentation, (C)

infringement of the other party's Intellectual Property Rights, or (D) matters for which liability cannot be excluded or limited under applicable law.

d. *Data Processing.* Except as otherwise expressly indicated in a written notice or Google documentation, no data processing terms (including the Cloud Data Processing Addendum) apply to Pre-GA Offerings and Customer should not use Pre-GA Offerings to process personal data or other data subject to legal or regulatory compliance requirements.

e. *Termination.* Either party may terminate Customer's use of a Pre-GA Offering at any time with written notice to the other party.

f. *EU Data Act Exclusion.* Google has no obligations under Chapter VI of the EU Data Act or the EU Data Act Terms below in respect of Pre-GA Offerings.

6. Google-Managed Multi-Cloud.

a. *Introduction.* The then-current services described as "Google-Managed Multi-Cloud Services" at <https://cloud.google.com/terms/services> ("Google-Managed MCS") are Google services, products and features that are hosted on the infrastructure of a third party cloud provider ("MCS Third-Party Provider"). While the Google-Managed MCS are not Services or Software, Customer's use of the Google-Managed MCS is subject to the terms of the Agreement applicable to Services (or Software, if applicable), as amended by this Section (Google-Managed Multi-Cloud).

b. *Admin Console.* The Google-Managed MCS may not be available through the Admin Console.

c. *MCS Third-Party Provider Relationship.*

(i) To make use of the Google-Managed MCS, Customer must maintain an independent agreement, account and billing relationship with the applicable MCS Third-Party Provider. The Agreement does not obligate Google or the MCS Third-Party Provider to provide the MCS Third-Party Provider's services that are necessary for the Customer to use the Google-Managed MCS.

(ii) If the MCS Third-Party Provider makes a change to its services or terms, and Google reasonably concludes that its provision of the Google-Managed MCS is no longer commercially feasible as a result of the change, Google may immediately Suspend all or part of Customer's use of the impacted Google-Managed MCS, or make any other discontinuance or backwards-incompatible change necessary to continue to provide the Google-Managed MCS. To the extent Google may Suspend or modify the Google-Managed MCS as set forth in this Section, the Google-Managed MCS are not subject to the Sections of the Agreement covering discontinuance and backwards-incompatible changes.

d. *Liability.* Notwithstanding anything to the contrary in the Agreement (except subject to any unlimited liabilities expressly stated in the Agreement), to the maximum extent permitted by law, each party's total aggregate Liability for damages arising out of or relating to the Google-Managed MCS is limited to the greater of (i) the Fees Customer paid for the Google-Managed MCS during the 12-month period before the event giving rise to liability and (ii) \$25,000.

e. *Disclaimer.* Notwithstanding anything to the contrary in the Agreement, the Google-Managed MCS are not (i) covered by any SLA, unless specifically



identified under the terms of the SLA, (ii) subject to any obligations for Google to provide termination or transition assistance or other technical assistance after Suspension or termination, and (iii) subject to any business continuity or disaster recovery commitments.

7. Benchmarking. Customer may itself (but may not permit a third party to): (a) conduct benchmark tests of the Services (each a "Test"); and (b) publicly disclose the results of such Tests only if (i) the public disclosure includes all necessary information to replicate the Tests, and (ii) Customer allows Google to conduct benchmark tests of Customer's publicly available products or services and publicly disclose the results of such tests. Notwithstanding the foregoing, Customer may not do either of the following on behalf of a hyperscale public cloud provider without Google's prior written consent: (A) conduct (directly or through a third party) any Test or (B) disclose the results of any such Test.

8. Trials. Certain Services may be made available to Customer on a trial basis ("Free Trial") subject to parameters and any Scope of Use, as presented in a Fees URL, Admin Console, Documentation, or otherwise. Use of a Free Trial indicates Customer's acceptance of any such parameters. If Customer is a government entity and is offered a Free Trial: (a) Customer represents and warrants that: (i) it is permitted to accept the Free Trial, (ii) its use of the Free Trial is not prohibited by applicable law or regulation, including any applicable anti-bribery, ethics, or conflict of interest rules and laws, and (iii) its use of the Free Trial will not prevent Google from bidding on, or otherwise participating in, other potential contracts issued by the government entity or its related bodies; (b) Customer may only use the Free Trial for official government purposes; and (c) Google has no expectation of payment or favorable treatment by offering the Free Trial.

9. User Experience Research. If Customer enrolls in the Google Cloud User Experience Research Program for Google Cloud Platform, Customer's participation will be subject to the Google Cloud User Experience Research Panel Addendum available at <https://cloud.google.com/terms/user-experience-research> or a successor URL.

10. PGSSI-S. Customer will comply with France's General Security Policy for Health Information Systems (PGSSI-S) to the extent applicable.

11. APIs and non-Google cloud services. Certain APIs and non-Google cloud services accessible through the Admin Console have separate terms or privacy policies. Notwithstanding any reference to the Google Cloud Terms of Service or the Google Cloud Privacy Notice in the Admin Console, the API-specific terms and privacy policies will apply to Customer's use of those APIs or services.

12. Resource Fields Data. Data included in Project Name, Project ID, or other resource fields do not constitute Customer Data. Do not include confidential, sensitive, or personally identifiable information in these fields.

13. Google Maps Content. Certain Services may incorporate features and content from Google Maps (“Google Maps Content”). If Customer provides its Google Maps Platform credentials to enable a Service to access Google Maps Content, such use or access is subject to the agreement under which Google has agreed to provide Google Maps Platform to Customer. Otherwise, Customer agrees that its use of or access to such Google Maps Content is subject to the then-current versions of the: (a) Google Maps/Google Earth Additional Terms of Service at https://maps.google.com/help/terms_maps.html; and (b) Google Privacy Policy at <https://www.google.com/policies/privacy/>.

14. Resold Customers. This Section 14 (Resold Customers) applies only if (a) Customer orders Google Cloud Platform Services from a Reseller under a Reseller Agreement (such Services, “Resold Services”) and (b) Customer has a direct agreement with Google to provision those Resold Services.

a. Additional Definitions.

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

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

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

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

b. Applicable Terms. For the purposes of Resold Services:

(i) The Section of the Agreement entitled “Payment Terms” will not apply, nor will any provisions in the applicable Service Specific Terms relating to billing, invoicing, or payment;

(ii) Reseller Fees will apply and be payable directly to Reseller, and all prices for Resold Services will be solely determined between Reseller and Customer;

(iii) Google will provide to Customer the Resold Services described in the Reseller Order to the extent that there is a valid and binding order for such Services between Google and Reseller;

(iv) Customer will receive any applicable SLA credits or monetary refunds described in this Agreement from Reseller only (and Customer must notify Reseller if Google fails to meet any SLA);

(v) Notwithstanding Google’s support obligations in the TSS Guidelines, Google will not provide any support to Customer unless (A) Customer orders TSS from Google directly or (B) Reseller orders TSS from Google on behalf of Customer, and such TSS entitlement requires Google to provide TSS directly to Customer. All other support (if any) will be provided to Customer by Reseller in accordance with the Reseller Agreement, subject to Section 14(e) (Reseller Technical Support);

(vi) Customer acknowledges that access to the Services may be Suspended if at any time Reseller or Customer fails to maintain a billing account linked to Customer’s Account;

(vii) In the event of termination of this Agreement, Google will send Reseller (and not Customer) the final invoice (if applicable) for payment obligations related to Resold



Services. Customer will notify (A) Reseller of any termination of this Agreement and (B) Google of any termination of the Reseller Agreement;

(viii) Any renewal(s) of the Resold Services and/or any Reseller Order will be as agreed between Customer and Reseller;

(ix) If Reseller fails to pay an undisputed invoice for Resold Services to Google due to Customer's failure to pay Reseller, Google may Suspend Customer's access to the Services;

(x) To the extent that any Customer Data is under Reseller's organizational resource, then notwithstanding anything to the contrary in this Agreement (including the Cloud Data Processing Addendum):

(A) the Cloud Data Processing Addendum will not apply with respect to the processing and security of such Customer Data;

(B) Google will only access, use, and otherwise process such Customer Data in accordance with the separate agreement between Google and Reseller (including its then-current terms describing data processing and security of "Partner Data" as defined by that agreement) and will not access, use, or process such Customer Data for any other purpose; and

(C) the consents and notices for which Customer is responsible under the section of this Agreement titled "Privacy" or "Consents" must also permit accessing, storing, and processing of Customer Data as described in subsection (B) above.

(xi) The Google Cloud Platform Services require linking to the Reseller's billing account in order to be billed by the Reseller. Customer acknowledges and agrees that, (A) if Google's agreement with the Reseller or Customer's Reseller Agreement is terminated or expires, then the Services will no longer be linked to the Reseller's billing account, and (B) unless any such Services used by Customer are linked to the Reseller's billing account, such Services will (x) not constitute Resold Services (and therefore not be subject to this Section 14 (Resold Customers)), and (y) be regarded as Services ordered directly from Google and accordingly, despite the terms of the Reseller Agreement (including the fees agreed between Customer and Reseller), Customer will be required to pay Fees to Google for such Services, in accordance with the terms of this Agreement.

(xii) "Cloud Data Processing Addendum", as it is used in this Agreement, means the then-current terms describing data processing and security obligations with respect to Customer Data that is under Customer's (not Reseller's) organizational resource, as described at <https://cloud.google.com/terms/data-processing-addendum>.

(xiii) "Order Term," as it is used in this Agreement, means the period of time starting on the Services Start Date or the renewal date (as applicable) for the Resold Services and continuing until the expiration or termination of the applicable Reseller Order; and

(xiv) "Services Start Date," as it is used in this Agreement, means either the start date described in the Reseller Order or, if none is specified in the Reseller Order, the date Google makes the Resold Services available to Customer; and

c. **Liability Cap.** For the purposes of the section of the Agreement titled "Limitation on Amount of Liability", where the event giving rise to Liability is a breach of this Agreement or otherwise arises in connection with the Resold Services, "Fees" as it is used in that Section means "Reseller Fees". If Customer or Google brings a claim under the Agreement, then, for the purposes of establishing the Liability cap under the section of the Agreement titled "Limitation on Amount of Liability", upon Google's

request, Customer will (i) promptly disclose to Google the amount of any Reseller Fees paid or payable under the Reseller Agreement; (ii) consent to Reseller disclosing such amount to Google, notwithstanding Reseller's confidentiality obligations under the Reseller Agreement; and (iii) procure any consents necessary to enable Customer's or Reseller's disclosure under this Section 14(c) (Liability Cap). Subject to the section of the Agreement titled "Unlimited Liabilities", Google will not be liable for damages under this Agreement to the extent Customer has claimed damages from Reseller in respect of the same event or series of events.

d. *Sharing Confidential Information.* Google may share Customer Confidential Information with Reseller as a Delegate subject to the section of the Agreement titled "Confidentiality" or "Confidential Information".

e. *Reseller-Customer Relationship.* At Customer's discretion, Reseller may access Customer's Account. As between Google and Customer, Customer is solely responsible for (i) any access by Reseller to Customer's Account; (ii) defining in the Reseller Agreement any rights or obligations as between Reseller and Customer with respect to the Resold Services; and (iii) verifying whether data provided to Google by Customer or End Users through the Resold Services under the Account, and data that Customer or End Users derive from that data through their use of the Resold Services, will be under Customer's or Reseller's organizational resource. Google will not have any Liability arising out of a Reseller's (A) suspension or termination of Customer's access to the Services; (B) access to and visibility of Customer's Account and Customer's Account's billing-related metadata; or (C) offering or provisioning of Reseller or third party products or services.

f. *Reseller Technical Support.* Customer acknowledges and agrees that Reseller may disclose Customer and End User personal data to Google as reasonably required for Reseller to handle any support issues that Customer escalates to or via Reseller.

15. Customer Data. Except to the extent expressly described in the Agreement or required by applicable law, Customer is responsible for all Customer Data, including securing and maintaining all applicable rights required for Customer's use of Customer Data.

16. EU Data Act Terms.

a. *Additional Definitions.* For purposes of this Section (EU Data Act Terms):

"*Completion Notice*" has the meaning given in Section 16(g) (Switching Initiation and Process) and takes effect as described in that Section.

"*Customer Account Information*" means information that is provided by Customer when creating the Account for use with the Google DP Service(s).

"*Customer Configurations*" means configurations and settings (including service and security settings for data) that are applied by Customer within the Google DP Service(s).

"*Customer Defined Attributes*" means resource identifiers, attributes and other data labels that are applied by Customer within the Google DP Service(s).

"*Data*" has the meaning given by the EUDA.

"*Data Processing Service*" (or "*DP Service*") has the meaning given by the EUDA.

"*Data Recovery Period*" means the period of at least 30 calendar days from the end of the Migration Period until termination of the Agreement or withdrawal of

Customer's Exit Notice under Section 16(g)(ii), as applicable in accordance with Section 16(g) (Switching Initiation and Process).

"*Digital Assets*" has the meaning given by the EUDA.

"*EUDA*" means Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

"*Exit Notice*" has the meaning given in Section 16(e) (Customer's Decision).

"*Exportable Data*" has the meaning given by the EUDA (notwithstanding references to specific articles of the EUDA in the EUDA definition).

"*Google DP Service*" means a DP Service provided by Google, as described at <https://cloud.google.com/terms/data-portability> (as may be updated from time to time).

"*Google Metadata*" means Google-generated metadata that is (a) directly related to Customer's use of the Google DP Service(s) and (b) required by Google to operate and maintain the Google DP Service(s) and by Customer to restore service functionalities in the infrastructure of a destination provider of DP Services or an On-Premises ICT Infrastructure.

"*Google Operational Data*" means Google-generated data (including metadata) that is (a) not directly related to Customer's use of the Google DP Service(s) and (b) derived from Google's systems and operation of the Google DP Service(s).

"*ICT*" means information and communication technology.

"*Initiation Period*" means the period of 30 calendar days from the end of the Intake Period.

"*Intake Period*" means the period of 14 calendar days from the date of Customer's submission of an Exit Notice.

"*Migration Period*" means the period of 30 calendar days from the end of the Initiation Period, as applicable in accordance with Section 16(g) (Switching Initiation and Process) and as may be extended in accordance with Section 16(h) (Extended Migration Period).

"*Month End*" means the last day of a calendar month.

"*Non-Personal Data*" has the meaning given by the EUDA.

"*On-Premises ICT Infrastructure*" has the meaning given by the EUDA.

"*Parallel DP Service*" means a DP Service offered by a different provider and procured by Customer for its own use in parallel with a Google DP Service.

"*personal data*" has the meaning given by the EU GDPR.

"*Processing*" has the meaning given by the EUDA.

"*Switching*" (or "*Switch*") has the meaning given by the EUDA.

"*Switching Charges*" has the meaning given by the EUDA.

"*Trade Secret*" has the meaning given by the EUDA.

b. *Application*. This Section applies only (i) if Customer's billing address is in the European Economic Area and (ii) in respect of the Google DP Service(s).

c. *Compliance with EUDA*. Both parties will comply with their obligations under the EUDA related to Switching from the Google DP Service(s), including cooperating in good faith as required by the EUDA.

d. *Customer's Right to Switch*. In accordance with this Section Customer may, upon request, Switch from a Google DP Service to a DP Service offered by a different provider and/or port all Exportable Data and Digital Assets to an On-Premises ICT Infrastructure without undue delay during the Initiation Period and Migration Period.

For clarity, this right to Switch will not prevent Customer from continuing to access the Google DP Service(s) during the Data Recovery Period as described in Section 16(g) (Switching Initiation and Process).

e. *Customer's Decision*. If Customer wishes to Switch from a Google DP Service as described in Section 16(d) (Customer's Right to Switch) during and/or after the Initiation Period and/or wishes to erase its Exportable Data and Digital Assets related to a Google DP Service(s) after the Initiation Period, Customer must first notify Google of Customer's decision by having a duly authorized representative submit the form at https://support.google.com/cloud/contact/cloud_exit (an "Exit Notice") and, if applicable, include the necessary details of any destination provider of DP Services.

f. *Google's Switching Obligations*. If Customer submits an Exit Notice as described in Section 16(e) (Customer's Decision), then Google will do the following during the Initiation Period, Migration Period, and Data Recovery Period, as applicable:

- (i) provide reasonable assistance to Customer and third parties authorised by Customer in the Switching process;
- (ii) act with due care to maintain business continuity and continue the provision of the Google DP Service(s) under the Agreement;
- (iii) provide clear information concerning known risks to continuity in the provision of the Google DP Service(s) under the Agreement, including via the dashboard at <https://status.cloud.google.com> and/or the dashboard Customer may choose to enable and configure via the Google DP Service(s) to access more specific information (both of which dashboards are provided for informational purposes only);
- (iv) maintain a continued high level of security throughout the Switching process, in particular for Exportable Data and Digital Assets during their export and during the Data Recovery Period, in accordance with applicable European Union or national law;
- (v) enable Customer, in a manner consistent with the functionality of the Google DP Service(s), to export the categories of Data and Digital Assets described in Section 16(g) (Switching Initiation and Process); and
- (vi) otherwise support Customer's exit strategy for the relevant Google DP Service(s), including by assigning a Google support agent during the Intake Period to coordinate Google's assistance with the Switching process and by providing all relevant information.

g. *Switching Initiation and Process*. If Customer submits an Exit Notice as described in Section 16(e) (Customer's Decision), then Customer will be responsible for initiating the Switching process (if applicable) during the Initiation Period with at least two (2) working days' prior notice to its assigned Google support agent, subject to the following:

- (i) if Customer has opted for only Switching as described in Section 16(e) (Customer's Decision) but does not initiate the Switching process in compliance with this Section by the end of the Initiation Period, then in relation to any Google DP Service(s) covered by Customer's decision:
 - (A) neither a Migration Period nor Data Recovery Period will apply;
 - (B) Customer will be deemed to have withdrawn its Exit Notice (without limiting Customer's ability to submit another one); and
 - (C) the Agreement will remain in force;
- (ii) If Customer has opted for Switching as described in Section 16(e) (Customer's Decision) and initiates the Switching process in compliance with this Section by the

end of the Initiation Period, then in relation to any Google DP Service(s) covered by Customer's decision:

(A) a Migration Period and Data Recovery Period will apply;

(B) the categories of Data and Digital Assets that can be exported during the Switching process are as follows:

a) Exportable Data comprising Customer Account Information, Customer Configurations, Customer Data and Google Metadata; and

b) Customer Applications;

(C) the categories of Data that are exempted from Exportable Data, without the exemption impeding or delaying the Switching process, are as follows:

a) Data specific to the internal functioning of the Google DP Service(s) that would, if exported, risk a breach of Google's Trade Secrets, namely Google Operational Data; and

b) Data related to the integrity and/or security of the Google DP Service(s) that would, if exported, expose Google to cybersecurity vulnerabilities;

(D) for clarity, Exportable Data excludes the following by definition:

a) Data not directly or indirectly generated or cogenerated by Customer's use of the Google DP Service(s); and

b) assets or Data protected by intellectual property rights, or constituting a Trade Secret, of Google or third parties;

(E) as between the parties and without limiting any of Google's obligations under this Section, Customer will be responsible for:

a) its storage of any copies of Data and Digital Assets (including Exportable Data) related to the Google DP Service(s) outside Google's or Google's Subprocessors' systems;

b) the security of any Data and Digital Assets (including Exportable Data) outside Google's and Google's Subprocessors' systems (including the security of Data and Digital Assets on systems managed or controlled by the destination provider of DP Services or on Customer's own infrastructure);

c) driving and managing the Switching process, in particular during the Initiation Period and Migration Period;

d) all acts and omissions of third parties engaged by Customer in relation to the Switching process;

(F) after the Migration Period:

a) Customer may no longer migrate workloads or production data (or otherwise consume networking resources) for Switching purposes, but may complete other aspects of the Switching process such as data retrieval;

b) Customer will:

(i) be responsible for notifying Google of Customer's successful completion of the Switching process by having a duly authorized representative submit the form at https://support.google.com/cloud/contact/cloud_exit_completion (a "Completion Notice") no earlier than the first day after the Migration Period and within 180 calendar days of the end of the Migration Period;

(ii) be deemed to have terminated the Agreement for convenience, a minimum of 30 calendar days after the date of Customer's submission of the Completion Notice, at the Month End following such minimum period; and

- (iii) if Customer fails to submit a Completion Notice within 180 calendar days of the end of the Migration Period, be deemed to have withdrawn its Exit Notice at the end of such 180-day period (without limiting Customer's ability to submit another one);
- c) Google will notify Customer of any such termination and, subject to Section 16(i) (Customer's Partial Exit), fully erase all Exportable Data and Digital Assets generated directly by Customer or relating to Customer directly in accordance with the Cloud Data Processing Addendum (as applicable);
- (G) Google will not impose any Switching Charges for the Switching process described in this Section; and/or
- (iii) If Customer has opted for erasure as described in Section 16(e) (Customer's Decision), then in relation to the Google DP Service(s) covered by Customer's decision:
 - (A) if Section 16(g)(ii) also applies, then:
 - a) a Migration Period and Data Recovery Period will apply as described in Section 16(g)(ii); and
 - b) erasure of Exportable Data and Digital Assets will be governed by Section 16(g)(ii); and
 - (B) if Section 16(g)(ii) does not also apply, then:
 - a) neither a Migration Period nor Data Recovery Period will apply;
 - b) Customer will be deemed to have terminated the Agreement for convenience at the end of the Initiation Period; and
 - c) Google will notify Customer of such termination and, subject to Section 16(i) (Customer's Partial Exit), fully erase all Exportable Data and Digital Assets generated directly by Customer or relating to Customer directly in accordance with the Cloud Data Processing Addendum (as applicable).
- h. *Extended Migration Period.* The Migration Period may be extended:
 - (i) once by Google, if Google believes a Migration Period of 30 calendar days is not technically feasible; notifies Customer during the Intake Period; and, in Google's notice, duly justifies the technical unfeasibility and defines an alternative Migration Period of no greater than 7 months; and
 - (ii) once by Customer, if Customer wishes to have a longer Migration Period for any reason; notifies its assigned Google support agent during the then-current Migration Period; and, in Customer's notice, defines an alternative Migration Period.
- i. *Customer's Partial Exit.* If, on the date of deemed termination of the Agreement in relation to the Google DP Service(s) under Section 16(g) (Switching Initiation and Process), Customer continues to use or order any other Services under the Agreement, Customer acknowledges that the Agreement will continue to apply to such other Services and agrees to defer full erasure under Section 16(g) (Switching Initiation and Process) of Exportable Data and Digital Assets related to the Google DP Service(s) until the Agreement terminates in its entirety.
- j. *Required Information.* Google will provide Customer with the following information and keep it up to date:
 - (i) information about available procedures for Switching and porting to and from the Google DP Service(s), including information about available Switching and porting methods and formats as well as restrictions and technical limitations known to Google, at <https://cloud.google.com/terms/data-portability>;

(ii) details of all data structures, data formats, relevant standards and open interoperability specifications available or applicable for the Exportable Data referred to in Section 16(g)(ii)(B) at <https://cloud.google.com/terms/data-portability>;

(iii) information about the jurisdictions to which the ICT infrastructure deployed for Data Processing of the Google DP Service(s) is or may be subject at <https://cloud.google.com/about/locations>, <https://cloud.google.com/vpc/docs/edge-locations>, <https://cloud.google.com/cdn/docs/locations> and <https://cloud.google.com/network-connectivity/docs/interconnect/concepts/colocation-facilities>; and

(iv) a general description of the technical, organisational, and contractual measures adopted by Google as provider of the Google DP Service(s) to prevent international governmental access to or the transfer of Non-Personal Data held in the European Union, where such access or transfer would conflict with EU or EU Member State law, in:

(A) the Cloud Data Processing Addendum, including Sections 7 (Data Security) and 11 (Subprocessors) of the General Terms, Appendix 2 (Security Measures) and the Google Cloud Platform section of Appendix 4 (Specific Products); and

(B) the remainder of the Agreement, including the sections entitled “Confidential Information” and “Representations and Warranties”.

k. *Agreement Duration; Separate Rights; Notices; Pre-GA Offerings.* For clarity:

(i) the Agreement will remain in effect, and Customer will be responsible for the Fees or Reseller Fees it incurs, until the effective date of termination of the Agreement in relation to the relevant Service(s);

(ii) nothing in this Section will limit Customer’s separate right to delete or export Customer Data in accordance with the Cloud Data Processing Addendum, to terminate the Agreement or to stop using a Google DP Service at any time;

(iii) all notices given under this Section must be in writing; and

(iv) Google has no obligations under Chapter VI of the EUDA or this Section in respect of Pre-GA Offerings.

l. *Interoperability.* Unless Customer has submitted an Exit Notice as described in Section 16(e) (Customer’s Decision) for the relevant Google DP Service, Customer may export Data from a Google DP Service to a Parallel DP Service as described at <https://cloud.google.com/data-transfer-essentials/docs/overview> (as may be updated from time to time), subject to the following:

(i) subsections (ii) and (iv) of Section 16(f) (Google’s Switching Obligations) and subsections (ii) (B), (C) and (D) of Section 16(g) (Switching Initiation and Process) will apply mutatis mutandis to facilitate interoperability for the purpose of such parallel use of DP Services; and

(ii) if Google imposes any data egress charges for such Data exports (as described at the above URL), Google may do so only for the purpose of passing on the egress costs incurred by Google, without exceeding such costs.

m. *Compliance Review.* Google may monitor or review the movement of Data or Digital Assets away from a Google DP Service to verify that Customer’s Switching process or Data export complies with this Section.

n. *Precedence.* To the extent of any conflict between:

(i) this Section and the EU GDPR, the EU GDPR will prevail with respect to personal data; and



(ii) this Section and Google's right to terminate the Agreement for an uncured material breach by Customer, Google's termination right will prevail.

o. *Transition; Availability of Terms.* Customer acknowledges that:

(i) this Section was made available prior to Customer's entry into the Agreement in relation to the Google DP Service(s) or that the Agreement was in force in relation to the Google DP Service(s) on 9 September 2025 when this Section was first published; and

(ii) Customer may store and reproduce this Section at any time by selecting "Expand all" at the top of <https://cloud.google.com/terms/service-terms> and then printing (and/or saving) all Service Specific Terms, including this Section, as a PDF.

17. Survival. The following Sections of these General Service Terms will survive expiration or termination of the Agreement: (a) Liability and the Disclaimer subsections in the Google-Managed Multi-Cloud Section and Pre-GA Offerings Terms; (b) Benchmarking; (c) the following subsections of the Resold Customers section: subsection (b)(vii); subsection (c) (Liability Cap); subsection (d) (Sharing Confidential Information); and subsection (e) (Reseller-Customer Relationship); and (d) Google's obligations under the EU Data Act Terms with respect to erasure of Exportable Data and Digital Assets.

Service Terms

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

Compute

1. App Engine - Data Location. Customer may configure App Engine to store Customer Data in the United States or European Union, and Google will store that Customer Data at rest only in that location. The Service does not limit the locations from which Customer or Customer End Users may access Customer Data or to which they may move Customer Data. For clarity, Customer Data does not include resource identifiers, attributes, or other data labels.

2. Google Cloud VMware Engine (GCVE).

a. *Definitions.* For the purposes of this Section:

"CA Software" means certain third-party software underlying GCVE, which includes VMware Cloud Foundation (VCF) software (for the avoidance of doubt, CA Software is not "Software" as defined in the Agreement); and

"CA, Inc." means CA, Inc. (the entity that licenses the CA Software), its applicable affiliate (such as Broadcom or VMware), or a successor entity to either of the foregoing.

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

c. *Usage Reporting.* Google may send certain information including usage metrics, location, and Customer's status as a GCVE customer to CA, Inc. This information will not include Customer Data.

d. *Service Restrictions.* Customer agrees to comply with all of the terms and conditions listed in <https://cloud.google.com/vmware-engine/docs> or a successor URL (as such terms and conditions may be updated by Google from time to time), including in the linked “Product Restrictions” page.

e. *CA Software.* In the course of using GCVE, Customer may have access to copies of the CA Software. Customer agrees that Customer will maintain the appropriate entitlements to use the CA Software (e.g., licenses from CA, Inc. to use the CA Software outside of GCVE).

f. *Licensing Portability Customers.* If Customer is using a GCVE SKU that supports CA Software licensing portability (as described in the Documentation), then Customer will (i) purchase an entitlement to the CA Software from CA, Inc. or a reseller of CA, Inc., and (ii) comply with all applicable sections of its agreement governing such purchase. Customer acknowledges and agrees that if Customer purchases such entitlements, then Google may restrict Customer’s access to GCVE upon instruction from CA, Inc., in which case (A) Google will have no liability to Customer (including no responsibility to return pre-paid Fees) for such restrictions and (B) Customer will still be responsible for all GCVE financial commitments.

g. *Prepaid 3-Year Committed Units.* Partners purchasing prepaid 3-year Committed Unit(s) (as defined in “Pricing and Billing Terms” below) for GCVE on or after July 18, 2024 may not use those Committed Unit(s) to make any multi-tenant CA, Inc. interfaces available to multiple customers.

h. *Aria Suite.* If Customer is using the “Aria Suite” in a self-managed capacity as part of Customer’s use of GCVE, Customer acknowledges and agrees that installation, configuration, maintenance, and security patching for the Aria Suite is Customer’s sole responsibility. Customer will ensure that the environment is maintained and patched in a timely manner after receiving patches and other updates from Google, including from a security standpoint (e.g., critical security patches). Further, Customer will enable Google to provide the support required for any use of Aria Suite. Google will not be responsible for any liability that ensues from Customer’s failure to comply with this Section.

i. *VMware Cloud Universal Program (“VMware Universal”).* VMware, Inc. (“VMware”) and VMware partners sell credits through VMware Universal that may be applied towards GCVE in accordance with Customer’s agreement with VMware. Customer’s purchase and use of GCVE through VMware Universal is subject to the Agreement and the following terms.

(i) The Agreement’s payment terms will not apply, and all fees will be payable to VMware and determined solely between VMware and Customer.

(ii) *Data Sharing with VMware.*

(A) Google may share with VMware information regarding Customer’s use of GCVE and Google Cloud Platform.

(B) Customer acknowledges that, to the extent Customer provides any data to VMware in connection with GCVE, VMware may share such data with Google to the extent reasonably required to provide GCVE (including technical support) and administer VMware Universal.

(C) If Customer brings a claim under the Agreement related to GCVE, Customer acknowledges that VMware may disclose to Google the fees or other amounts paid or payable by Customer to VMware for GCVE, and any other terms of the agreement



between Customer and VMware regarding GCVE or either party's performance under that agreement.

(iii) *Remedies*. Customer will seek any applicable SLA credits and monetary remedies described in the Agreement from VMware (and will not do so from Google).

(iv) *Support*. Google will provide technical support to Customer in accordance with the Agreement. Support fees for GCVE may be charged by VMware to Customer.

(v) *Financial Commitments*. If Customer has made financial commitments in an Order Form or addendum to the Agreement, then Google may apply Customer's GCVE consumption (at a rate determined by Google), or a portion of the applicable fees Google receives from VMware, to those commitments.

j. *Termination*. Customer agrees that if Customer materially breaches either (i) this Section or (ii) any other provision of the Agreement with respect to GCVE, then Google may, at its discretion, opt to exercise its "Termination for Breach" or "Termination for Cause" right under the Agreement with respect to GCVE only, in which case Customer may no longer access GCVE but may still access other Services.

3. BigQuery.

a. **ODBC/JDBC Drivers**. The ODBC and JDBC drivers for BigQuery (described here) are "Software" as defined in the Agreement and their use is subject to the "General Software Terms." These drivers may only be used with BigQuery.

b. Sharing (Analytics Hub)

(i) *Introduction*. Sharing in BigQuery (formerly known as Analytics Hub) helps customers publish and share sets of Customer Data ("Datasets") with other BigQuery customers as subscribers. Datasets are organized into shared repositories ("Exchanges") with each Dataset's listings including additional listing information ("Listing Materials") managed by the administrator of that Exchange ("Exchange Administrator").

(ii) *Exchange Administrators*. When acting as an Exchange Administrator: (A) Customer Listing Materials are considered Customer Data and (B) Customer is responsible for any Datasets listed in its Exchange, including handling takedown requests and securing necessary rights and consents.

(iii) *Disclaimer*. Google is not responsible for and will have no liability for (A) any terms or relationships between Customer and any third party or (B) any Datasets.

4. Looker Studio.

This Agreement only applies to (a) Looker Studio Pro or (b) Looker Studio if Customer has selected it to govern in the Admin Console.

5. Google Earth Engine.

a. *Non-Commercial Use*. Use of the free, non-commercial / research activities edition of Google Earth Engine is subject to the terms at <https://earthengine.google.com/terms/> or a successor URL, which may be updated by Google periodically.

b. *Incorporation into Applications*. Customer may not allow End Users of Customer's Applications to directly access or interact with the Google Earth Engine APIs unless those End Users have their own Google Cloud Platform Accounts and have access to Google Earth Engine from those Accounts.

6. Compute Engine.

a. *Future Reservations.* Customer may request a future reservation, as described at <https://cloud.google.com/compute/docs/future-reservations> (or a successor URL), by following the instructions at that URL. Google will determine in its sole discretion whether to approve each future reservation request, and approval will not be unreasonably withheld or delayed. Reserved VMs may not be transferred or shared amongst multiple customers by Customer (if the Customer is a reseller or supplier of Google Cloud Platform).

Networking

7. Cloud Interconnect

a. **Partner Interconnect.** Customer will independently engage a network service provider who has agreed with Google to supply connectivity between Customer and Google under Google's partner terms for Partner Interconnect. Google is not responsible for any issues arising outside of Google's network.

b. **Cross-Site Interconnect (CSI).** Notwithstanding any telecommunications restrictions in the Agreement, Customer may use CSI only in the countries listed at <https://cloud.google.com/network-connectivity/docs/interconnect/concepts/cross-site-locations>. In order for Customer to use CSI, Customer must establish Dedicated Interconnect presence with Google Cloud and may only use CSI in combination with that Dedicated Interconnect service offering. To the extent that Customer's use of CSI is subject to a Legal Process requesting Customer Data, Google will not be responsible for responding and Customer must directly respond to those requests.

8. Cloud NGFW and Cloud Intrusion Detection System (Cloud IDS).

Notwithstanding anything to the contrary in the "Benchmarking" section of the General Service Terms of these Service Specific Terms, Customer will not, and will not allow End Users to, disclose, publish, or otherwise make publicly-available any benchmark, or performance or comparison tests that are run on either the edition of Cloud NGFW titled "Cloud NGFW Enterprise" or Cloud IDS and that are conducted by Customer or an End User (or a third party authorized by Customer or an End User).

9. **Network Connectivity Center (NCC).** Notwithstanding any telecommunications restrictions in the Agreement, Customer may use NCC only in the countries listed at <https://cloud.google.com/network-connectivity/docs/network-connectivity-center/concepts/locations>. In order for Customer to use NCC, Customer must establish Virtual Private Cloud (VPC) presence with Google Cloud and may only use NCC in combination with that VPC service offering.

10. Spectrum Access System.

a. *Governing Agreement.* This Section 10 (Spectrum Access System) only applies to Customers procuring SAS under the terms of this Agreement.

b. *Additional Customer Obligations.* Customer is solely responsible for (i) the installation, operation, maintenance, and repair of Registered CBSDs; (ii) staffing, instructing, and managing personnel performing the installation, operation,

maintenance, and repair of Registered CBSDs; (iii) ensuring that such personnel are certified by WInnForum to the extent required by applicable law; and (iv) procuring and maintaining connectivity with Spectrum Access System to enable the ordering and registration of CBSDs and the use of Registered CBSDs. For clarity, Section 2(b) (Operations of Communications Services) in the General Services Terms of these Service Specific Terms does not prohibit Customer from using Spectrum Access System in compliance with this Section 10 (Spectrum Access System).

c. *Applicable Law.* Spectrum Access System is subject to Federal Communications Commission (“FCC”) regulations. Each party will comply with the rules and implementing orders of the FCC (including 47 C.F.R. Part 96), the Department of Defense, and the National Telecommunications and Information Administration, along with the duly adopted Release 1 standards of WInnForum, to the extent applicable to that party’s provision, receipt, or use of Spectrum Access System.

d. *No Personal Data.* Except for any Customer Account Information that may include personal data, Customer will not provide any CBSD Endpoint User Information or other regulated data to Google through Customer’s use of Spectrum Access System.

e. *Definitions.*

“*CBSD*” means a device with a radio access point that is certified by the FCC to operate in the Citizens Broadband Radio Services band.

“*CBSD Registration Information*” means data relating to the location, identification, operating parameters, and other aspects of Registered CBSDs.

“*CBSD Reporting Data*” means the anonymized or aggregated data and metadata Google receives from the Registered CBSDs during Customer’s use of Spectrum Access System.

“*CBSD Endpoint*” means a device that may establish wireless connectivity with the authorization of a Registered CBSD.

“*CBSD Endpoint User*” means an individual that uses any CBSD Endpoint.

“*CBSD Endpoint User Information*” means any information, data, or content relating to a CBSD Endpoint User, including (i) billing and usage information, passwords, and PINs; (ii) *transmitted* or received content information; (iii) authentication information and any other demographic information; and (iv) other information in connection with use by a CBSD Endpoint User of a CBSD Endpoint on any Registered CBSD or network of Registered CBSDs (excluding any information that may qualify as CBSD Registration Information or CBSD Reporting Data).

“*Customer Account Information*” means information provided by Customer in connection with the registration of CBSDs, which information consists of (i) contact and account information for Customer; (ii) identification information for all Registered CBSDs registered to Customer, as prescribed by WInnForum standards; (iii) identifying information for all groups of CBSDs for Customer; and (iv) information relating to Customer’s priority access licenses (as applicable), including identification numbers, boundary information, protection area, CBSD cluster lists, grouping information, and any leases of such priority access licenses.

“*Registered CBSD*” means a CBSD that is registered with Google and operated by Customer via Spectrum Access System.

“*WInnForum*” means the Wireless Innovation Forum or any successor organization.

Developer Tools

11. Assured Open Source Software (AOSS). TSS is not available for free tiers of AOSS.

12. Google Device Cloud.

a. *License Agreement.* Customer's access to and use of a Device Partner's testing device or the Partner Device Lab itself through Google Device Cloud is governed solely by the license agreement between Customer and the Device Partner. By enabling the Partner Device Lab or by accessing any Device Partner testing device through the Google Device Cloud service, Customer accepts the license agreement terms presented at the time of initial access and instructs Google to share Customer Data with that Device Partner for use by the Device Partner for the sole purpose of executing development tests. Customer acknowledges that Device Partners are not acting as Google's subprocessors, and as such any Customer Data that is shared with a Device Partner will be processed in accordance with that Device Partner's data processing terms (and not the Cloud Data Processing Addendum). Customer acknowledges that Google exercises no control over the operation or location of Partner Device Labs offered through Google Device Cloud and is not responsible or liable for Device Partner's actions, labs or devices.

b. *Definition(s).*

"*Device Partner*" means a device manufacturing company that maintains a lab of Android-based devices for purposes of connecting to the Google infrastructure.

AI / ML Services

13. Definitions.

"*AI Agents*" are goal-oriented, AI systems or workflows that perform actions or tasks on behalf of Customer in a supervised or autonomous manner that Customer may create, orchestrate, or initiate within an Agentic AI Service.

"*Customer Adapter Model*" means an adapter model that Customer creates using its Customer Data with an AI/ML Service.

"*Customer Model*" means (i) a model that Customer creates without using a Google Pre-Trained Model or (ii) a model owned by Customer that Customer uploads, fine tunes, or deploys in AI/ML Services. Customer Models do not include Customer Adapter Models.

"*Fine-Tuned Google Model*" means an uptrained model that Customer creates by using an AI/ML Service to retrain or fine-tune a Google Pre-Trained Model using Customer Data.

"*Google Customer-Trained Model*" means a model trained or retrained by Customer that leverages Google's pre-existing intellectual property using an AI/ML Service and not released as an open model under an open source or other license.

"*Google Models*" means Google Pre-Trained Models, Fine-Tuned Google Models, and Google Customer-Trained Models.

"*Google Pre-Trained Model*" means a model trained by Google and not released as an open model under an open source or other license.

"*Separate Offering*" means a model, dataset, application, product, service, solution, AI Agent or any other offering that Google makes available for a Customer's use with AI/ML Services that is subject to terms and conditions separate from the Agreement, such as an open source license, third party terms, or other terms.

14. Intellectual Property Terms for AI/ML Services.

- a. *Non-Google Models.* As between Customer and Google and in connection with use of an AI/ML Service (as described at <https://cloud.google.com/terms/services>), Google does not assert any ownership rights in (i) Customer Models, (ii) Customer Adapter Models, or (iii) Separate Offerings, each to the extent they do not contain any pre-existing Google intellectual property.
- b. *Google Models.* Customer will have sole access to use Fine-Tuned Google Models and Google Customer-Trained Models. Neither Google nor any third party not authorized by Customer may access or use Fine-Tuned Google Models and Google Customer-Trained Models, including after expiration or termination of the Agreement. Google owns all Intellectual Property Rights in Google Models. Where permitted by the AI/ML Service, any exported Fine-Tuned Google Model is licensed as Software.

15. AI/ML Data Location. Customer may configure the Services listed at <https://cloud.google.com/terms/data-residency> to (a) store Customer Data at rest and (b) perform machine learning processing of Customer Data by the Service, in each case in a specific Multi-Region, and Google will perform (a) and (b) only in that Multi-Region. For clarity, Customer Data does not include resource identifiers, attributes, or other data labels.

16. Use Restrictions for AI/ML Services.

- a. *Competitive Use.* Customer will not, and will not allow End Users to use an AI/ML Service or Generated Output to develop a similar or competing product or service. Google may immediately suspend or terminate Customer's use of any AI/ML Service based on any suspected violation of the preceding sentence. This restriction does not apply to Vertex AI Platform so long as Customer does not use a Google Pre-Trained Model.
- b. *Model Restrictions.* Customer will not, and will not allow End Users to, use output from an AI/ML Service (including Generated Output) to: (i) substitute, replace, or circumvent the use of a Google Model, directly or indirectly, or (ii) create or improve models similar to a Google Model. However, if an AI/ML Service offers the feature of fine-tuning, Customer may use output from that AI/ML Service (including Generated Output) to create and use Fine-Tuned Google Models instead of Google Pre-Trained Models.
- c. *No Reverse Engineering.* Customer will not, and will not allow End Users to, reverse engineer or extract any components of an AI/ML Service, Software, or its models (such as using prompts to discover training data). Google may immediately suspend or terminate Customer's use of any AI/ML Service based on any suspected violation of the preceding sentence.

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

18. Separate Offerings and Customer Models.

- a. *Use of Separate Offerings on the Google Cloud Platform.* Customer's use of Separate Offerings is subject to separate terms and conditions.

b. *Disclaimer and Indemnity.* Google disclaims all liability arising from Customer's use of Separate Offerings and Customer Models, and Google's indemnification obligations do not apply to allegations arising from Separate Offerings or Customer Models.

19. **Generative AI Services.**

a. *Definition.* "Generated Output" means the data or content generated by a Generative AI Service prompted by Customer Data. Generated Output is Customer Data. As between Customer and Google, Google does not assert any ownership rights in any new intellectual property created in the Generated Output.

b. *Disclaimer.* **Generative AI Services (as described at <https://cloud.google.com/terms/services>) use emerging technology, may provide inaccurate or offensive Generated Output, and are not designed for or intended to meet Customer's regulatory, legal, or other obligations. Customer acknowledges that a Generative AI Service may, in some scenarios, produce the same or similar Generated Output for multiple customers.**

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

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

e. *Healthcare Restrictions.* Customer will not, and will not allow End Users to, use the Generative AI Services for clinical purposes (for clarity, non-clinical research, scheduling, or other administrative tasks is not restricted), as a substitute for professional medical advice, or in any manner that is overseen by or requires clearance or approval from any applicable regulatory authority.

f. *Suspected Violations.* Google may immediately suspend or terminate Customer's use of a Generative AI Service based on any suspected violation of Section 16(b) or subsection (d) above.

g. *Restrictions.* The restrictions contained in subsections (d) and (e) above are deemed to be "Restrictions" or "Use Restrictions" under the applicable Agreement.

h. *Handling of Prompts and Generated Output.* Absent Customer's prior permission or instruction, Google will not store outside Customer's Account (i) Customer Data prompted to a Generative AI Service for longer than is reasonably necessary to create the Generated Output, or (ii) the Generated Output.

i. *Additional Google Indemnification Obligations.*

(i) *Generated Output.* Google's indemnification obligations under the Agreement also apply to allegations that an unmodified Generated Output from a Generative AI Indemnified Service using only Google Pre-Trained Model(s), a Fine-Tuned Google Model, or a Customer Adapter Model used with a Google Pre-Trained Model infringes a third party's Intellectual Property Rights. This subsection (i) (Generated Output) does not apply if the allegation relates to a Generated Output where: (1) Customer creates or uses such Generated Output that it knew or should have known was likely infringing, (2) Customer (or Google at Customer's instruction) disregards, disables, modifies, or circumvents source citations, filters, instructions, or other tools Google makes available to help Customer create or use Generated Output

responsibly, (3) Customer uses such Generated Output after receiving notice of an infringement claim from the rightsholder or its authorized agent, (4) the allegation is based on a trademark-related right as a result of Customer's use of such Generated Output in trade or commerce, or (5) Customer does not have the necessary rights to the Customer Data used to customize or retrain the Fine-Tuned Google Model or Customer Adapter Model, or customize such Generated Output using a Generative AI Service. "Generative AI Indemnified Service" means a Service or feature listed at <https://cloud.google.com/terms/generative-ai-indemnified-services>, where the use of such Service or feature is not provided to Customer free of charge.

(ii) *Training Data*. Google's indemnification obligations under the Agreement also apply to allegations that Google's use of training data to create any Google Pre-Trained Model utilized by a Generative AI Service infringes a third party's Intellectual Property Rights. This indemnity does not cover allegations related to a specific Generated Output, which may be covered by subsection (i) (Generated Output) above.

j. *Modifying, Disregarding, or Disabling Safety Filters*. Google makes available safety filters for certain Generative AI Services. Customer is solely responsible for (i) its use, non-use, or modification (including modifications made by Google at Customer's instruction) of safety filters in creating Generated Output, and (ii) disregarding safety instructions or Documentation.

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

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

1. Will only use Grounding with Google Search in a Customer Application that is owned and operated by the Customer and will only display the Grounded Results with the associated Search Suggestion(s) to the End User who submitted the prompt.
2. Will not, and will not allow its End Users or any third party to, cache, frame, syndicate, resell, analyze, train on, or otherwise learn from Grounded Results or Search Suggestions. For clarity, Grounded Results, Search Suggestions, and Links are intended to be used in combination to respond to a given End User prompt and it is a violation of these terms to use Grounding with Google Search to extract or collect one or more of these components for another purpose (for example, using programmatic or automated means to collect Links, using Links to build an index, or using Links to identify destination pages for crawling or scraping).

3. Will not, and will not allow its End Users or any third party to, copy, store, or implement any click tracking, Link-tracking or other monitoring of Grounded Results or Search Suggestions, except that:

- Customer may copy and store, for up to two (2) years the Grounded Results:
 - (1) that were displayed by Customer only to evaluate and optimize the display of the Grounded Results in the Customer Application;
 - (2) in the chat history of an End User of the Customer Application only for the purpose of allowing that End User to view their chat history.
- Customer may copy and store the Grounded Result and Search Suggestions only for the purpose of and for the minimum time necessary to comply with applicable law or regulations.
- Customer may allow its End Users to copy and store individual Grounded Results that Customer displayed to that End User through the Customer Application as long as Customer does not allow Grounded Results to be: (i) accessed or collected by automated or programmatic means, or (ii) to be used to create a database.
- Customer may monitor End User interactions with their Customer Application interface, however, Customer will not track whether those interactions were specifically with a given Search Suggestion or Grounded Result (in each case, in whole or in part, including any specific Links).

4. Unless permitted by Google in writing (including in the Documentation):

- will not modify, or intersperse any other content with, the Grounded Results or Search Suggestions; and
- will not place any interstitial content between any Link or Search Suggestion and the associated destination page, redirect End Users away from destination pages, or minimize, remove, or otherwise inhibit the full and complete display of any destination page.

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

(iii) *Guidelines.* If Customer builds an external-facing Customer Application, the Client Application Guidelines apply to the Customer's use of Grounding with Google Search. For purposes of the Client Application Guidelines, Customer Applications that are using Grounding with Google Search are considered Approved Applications.

(iv) *Survival.* This subsection "Grounding with Google Search" will survive termination or expiration of the Agreement, as applicable.

l. *Web Grounding for Enterprise.* Section 19(k) (Grounding with Google Search) also applies to Web Grounding for Enterprise, except that: (i) all references to 'Grounding with Google Search' are replaced with 'Web Grounding for Enterprise', (ii) in the "Grounded Results" definition, the phrase 'Google's search engine' is replaced with 'GCP's web index', and; (iii) subsection 19k(ii) is deleted.

m. *Grounding with Google Maps.* "Grounding with Google Maps" is a generative AI feature of the Generative AI on Vertex AI Service that provides Grounded Results. "Google Maps Grounded Results" mean responses that Google generates using Google Maps Data in response to an End User initiated prompt. "Google Maps Data" means the content originating from Google Maps in the Google Maps Grounded

Results, including in the output text, in the metadata of the Google Maps Grounded Results, in the Google Maps Links, and content accessed through Google Maps Links. “Google Maps Links” mean the URLs that Google provides in a Google Maps Grounded Result and any titles or labels provided with those URLs. If Google Maps Links are clicked on, these separate Google Maps End User Terms (https://maps.google.com/help/terms_maps/) and the Google Privacy Policy (<https://policies.google.com/privacy>) govern the destination page. Google Maps Data in the text of a Google Maps Grounded Result will be identified via the Google Maps Links. Google Maps Grounded Results are Generated Output. Notwithstanding anything to the contrary in the Agreement, Google and its content providers retain all rights to Google Maps Data.

(i) *Use Restrictions for Grounding with Google Maps. Customer:*

1. Will only use Grounding with Google Maps in a Customer Application that is owned and operated by Customer and will only use Grounding with Google Maps to display the Google Maps Grounded Results with the associated Google Maps Links to the End User who initiated the prompt.
2. Will not modify the Google Maps Grounded Result or intersperse any other content with the Google Maps Grounded Result, place any interstitial content between the text of the Google Maps Grounded Result and the Google Maps Links or the Google Maps Links and the associated destination page, or redirect End Users away from the destination pages or minimize, remove, or otherwise inhibit the full and complete display of any destination page.
3. Will comply with the Documentation.
4. Will not, and will not allow its End Users or any third party to:
 - (a) cache or store Google Maps Grounded Results except that Customer may cache or store Google Maps Grounded Results:
 - (i) for up to ninety (90) days, only to evaluate and optimize the display of the Google Maps Grounded Results for the Customer Application; or,
 - (ii) in the chat history of an End User of the Customer Application for up to six (6) months for the purpose of allowing that End User to view their chat history or to maintain prior conversation context for that End User within the Customer Application;
 - (b) scrape any Google Maps Data;
 - (c) use Google Maps Grounded Results for High Risk Activities, including activities such as emergency response services; and
 - (d) distribute or market any Customer Applications in any Prohibited Territory as defined in the Documentation.
- (ii) *Storage for Debugging and Testing.* Customer acknowledges that it is reasonably necessary for Google to store prompts, contextual information that Customer may provide, and Generated Output for thirty (30) days for the purposes of creating Google Maps Grounded Results, and since such information is being stored, Customer instructs Google that the stored information can be used for debugging and testing of systems that support Grounding with Google Maps.

n. *Agentic AI Services.*

- (i) Customer is solely responsible for: (a) the actions and tasks performed by an Agentic AI Service or AI Agent; (b) determining whether the use of an Agentic AI Service or AI Agent is fit for its use case; (c) authorizing an Agentic AI Service or AI Agent’s access and connection to data, applications, and systems; and (d)

exercising judgment and supervision when and if an Agentic AI Service or AI Agent is used in production environments to avoid any potential harm the Agentic AI Service or AI Agent may cause.

(ii) The actions or tasks that an AI Agent performs are not Generated Output.

(iii) When using Grounding with Google Search in Gemini Enterprise or Agentspace, Section 19(k) (Grounding with Google Search) applies, provided that where Customer's use is in the Service's UI only, Section 19(k) is amended as follows:

(A) Subsections 19(k)(i)(1), (3), and (4) are deleted in their entirety and the first sentence of 19(k)(i)(2) is replaced with the following: "Customer will not, and will not allow its End Users or any third party to, copy, implement any click tracking, Link-tracking or other monitoring of, syndicate, resell, analyze, train on, or otherwise learn from Grounded Results or Search Suggestions."

(B) Subsection 19(k)(iii) (Guidelines) is deleted in its entirety.

o. *Provisioned Throughput*. Provisioned Throughput is a feature of the Vertex AI API. If Customer uses Provisioned Throughput, Google will use commercially reasonable efforts to prioritize Customer's throughput for its API calls to the designated models available through Generative AI on Vertex AI. Notwithstanding any other provision of the Agreement related to product discontinuation, Google may discontinue Provisioned Throughput for any model available through Generative AI on Vertex AI by providing Customer at least 6 months' prior notice, with no notice required if Google replaces such functionality with materially similar functionality.

20. Vertex AI Search and Gemini Enterprise. With respect to these Services, Customer may use only Customer Data and web domains that it owns or is authorized to utilize.

21. Vertex AI Studio. With respect to this Service's integration with YouTube, Customer may use only Customer Data and Content (as defined in the YouTube Terms of Service) (<https://www.youtube.com/static?template=terms>) that it owns or is authorized to use through the YouTube integration feature.

22. Celebrity Recognition. Customer will use celebrity recognition functionality in Cloud Vision and Video Intelligence API on celebrities, only with professionally-filmed media content that Customer owns or is authorized to use, and not for any surveillance-based purpose.

23. Customer Engagement Suite (formerly Contact Center AI (CCAI) Platform).

a. *No Access to Emergency Services*. Customer Engagement Suite includes Contact Center as a Service (CCaaS). CCaaS does not function as a telephonic or other communication service. The Service cannot send or receive emergency calls or texts, and will not be used for emergency services.

b. *Bring Your Own Carrier ("BYOC")*. In the BYOC model, Customer is responsible for obtaining telephony services from a third party and for all associated costs. Customer and its telephony provider are solely responsible for compliance with any regulatory and licensing requirements for such telephony services.

24. Cloud Translation API. Customer will comply with the HTML Markup Requirements found at <https://cloud.google.com/translate/markup> and the attribution requirements found at <https://cloud.google.com/translate/attribution>.

25. Speech on Device (SOD) / Automotive AI Agent (AAA) Premium Software. Customer's license to the Premium Software components of SOD and AAA is limited to using the Premium Software locally on activated, designated devices. Only Customers who subscribe to TSS are eligible to receive updates to the Premium Software. Upon termination or expiration of Customer's Order Form for SOD/AAA, Customer will permanently delete the Premium Software and associated SOD/AAA models (except those models on already-activated devices) and may not use SOD/AAA to perform any additional activations or distribute any more devices. Notwithstanding anything to the contrary in the "License" subsection of the "General Software Terms" above, the following apply:

- a. Customer may sublicense the Premium Software included as part of SOD/AAA to the extent necessary for using it on End User devices;
- b. Customer's license to such Premium Software will be perpetual to the extent that it remains on any device after the Term.

26. Automotive AI Agent. Automotive AI Agent models created by Customer based on Google Pre-Trained Models are Fine-Tuned Google Models as defined in these Service Specific Terms.

27. Visual Inspection AI. Customer may only download from Visual Inspection AI containerized Solution Artifacts (as described in the Documentation and licensed as Software) for the duration and number of cameras designated when downloaded by Customer in the Admin Console.

28. Retail Search. If Customer provides results for any query in a different order than the ranked order returned by Retail Search ("Alternative Ranking"), then (a) Google will not provide any support (including TSS) in relation to this Alternative Ranking and (b) Customer forfeits any rights granted by Google to use Google Brand Features in connection with Retail Search.

29. Anti Money Laundering AI. The Service may only be used for Customer's (or its own customers') detection of money-laundering activities as part of an anti money laundering (AML) compliance program. Customer will comply with the service limits defined in the Documentation and ensure that Service outputs are subject to human oversight, investigation, and evaluation by trained AML compliance personnel. Google may suspend or terminate Customer's use of the Service based on any suspected violation of the foregoing obligations.

30. Gemini Enterprise and Gemini for Government.

- a. *Additional Products.* Google makes optional Additional Products available to Customer and Customer End Users through Gemini for Government and Gemini Enterprise. Customer's use of Additional Products is subject to the Google Terms of Service available at <https://policies.google.com/terms> which are incorporated by reference into the Agreement and which may be updated by Google from time to

time, and any other terms of service Google makes available for a particular Additional Product. Additional Products may be enabled or disabled through the Admin Console.

b. *"Additional Products"* means products, services and applications that are not part of the Services but that may be accessible for use in conjunction with the Services. "Flow", "Project Mariner", and "Whisk" are Additional Products accessible via Gemini for Government and Gemini Enterprise.

Storage

31. Persistent Disk.

a. *Hyperdisk Exapools*. Customer and Google will work together in good faith to select the appropriate Zones (as defined at <https://cloud.google.com/compute/docs/regions-zones>) for Hyperdisk Exapool clusters. Customer acknowledges and agrees that once a Hyperdisk Exapool cluster is deployed to a particular Zone, Customer may not move it to another Zone without written agreement from Google.

Data Analytics

32. **Looker (Google Cloud core)**. If Google's measurement tools are unable to confirm Customer's usage of the Services, then (a) within 30 days of Google's request, Customer will provide a sufficiently-detailed written report describing usage of the Looker (Google Cloud core) Service by Customer and End Users during the requested period, and (b) Customer will provide reasonable assistance and access to information to verify the accuracy of Customer's usage report(s).

API Management

33. **Apigee**. Customer acknowledges and agrees that Customer will be charged overage Fees for usage of the Services in excess of Customer's subscription amount. If Customer is using Apigee Edge Team or Apigee Edge Business, the Fees for these overages are listed at <https://cloud.google.com/apigee/pricing/edge-overage>.

Bare Metal

34. Bare Metal Solution.

a. **Liability**. Notwithstanding anything to the contrary in the Agreement (except subject to any unlimited liabilities expressly stated in the Agreement), to the maximum extent permitted by law, each party's total aggregate Liability for damages arising out of or relating to Bare Metal Solution is limited to the greater of (i) the Fees Customer paid for Bare Metal Solution during the 12 month period before the event giving rise to liability and (ii) \$25,000. This Section will survive expiration or termination of the Agreement.

b. *Bare Metal Solution Proof of Concepts*. Customer may not use Bare Metal Solution proof of concepts and trials in connection with any production workloads.

Migration

35. Transfer Appliance Service.

a. *Trade Compliance.*

(i) In case of cross-border shipments of Appliance Materials, Customer may be responsible for export clearance and licensing (if applicable). Appliance Materials may be dual-use goods (including under Export Control Number 5A002) and subject to export restrictions. Google may designate a carrier to act as Customer's agent with the relevant customs and tax authorities to import or export the Appliance Materials, and Customer will cooperate with Google and its carrier, including providing export classification information and acting as the importer or exporter of record. Customer will not ship Appliance Materials except as authorized in writing by Google.

(ii) Without limiting Customer's obligation to comply with all laws applicable to its receipt or use of Appliance Materials (including any prohibitions on exporting, re-exporting or transferring Appliance Materials to comprehensively embargoed United States countries and regions), Customer may not export, re-export or transfer Appliance Materials to Russia or for use in Russia except as authorized in writing by Google.

b. *Responsibility for Appliance Materials.* While Appliance Materials are in its control, Customer is responsible for any loss or damage and will use appropriate security measures to protect them.

c. *Sole Remedy.* Customer's sole remedy in connection with any unsuccessful attempt to complete the Transfer Appliance Service is for Google to use reasonable efforts to re-perform the Transfer Appliance Service.

The Service Specific Terms for the Transfer Appliance Service are also applicable to Google Distributed Cloud connected Appliance Service excluding the "Sole Remedy" subsection above.

"*Appliance Materials*" means the materials provided by Google or its Subprocessors in connection with the Transfer Appliance Service or the Google Distributed Cloud connected Appliance Service, as applicable, including hardware and software.

Security and Identity

36. Assured Workloads.

a. *General.* Google will provide TSS for Assured Workloads in accordance with Customer-selected controls. It is Customer's responsibility to determine whether Customer-selected Admin Console controls are adequate for Customer's purposes.

b. *Assured Workloads Data Location.* If Customer is using Assured Workloads and configures any Service listed in the "Assured Workloads" section of <https://cloud.google.com/terms/data-residency> for data location as described in the General Service Terms Section 1 (Data Location), then in addition to Google's data location commitments under that Section 1 (Data Location), Google will process Customer Data in use by the configured Service (not including in any user interface) only within the country of the selected Region or within the country or countries of the selected Multi-Region (as applicable). If the selected Region or Multi-Region is located in the European Union, Google will process Customer Data in use by the

configured Service only within the European Union (but not necessarily in the same country).

Further, Assured Workloads enables Customer to prevent Google personnel located outside the Customer-selected Region or Multi-Region from accessing Customer Data in an Assured Workloads environment, as specified in the Documentation.

c. *ITAR Data*. Notwithstanding any restriction on the access or use of the Services for materials or activities subject to ITAR in the Agreement, Customer may access or use the Services with software or technical data subject to ITAR if Customer uses Assured Workloads Services explicitly identified in the Documentation as being compatible with ITAR requirements.

d. *Federal Risk and Authorization Management Program (FedRAMP) and Department of Defense Cloud Security Requirements Guide (DoD SRG)*. Certain Google Services have received FedRAMP or DoD SRG Authority to Operate (“ATO”) for defined Services. FedRAMP ATO Services are currently described at <https://cloud.google.com/security/compliance/fedramp> and DoD SRG ATO Services are currently described at <https://cloud.google.com/security/compliance/disa>. Customers are responsible for complying with the relevant FedRAMP and SRG requirements when using the Services, including the requirements in the Customer Responsibility Matrix (“CRM”). The CRM is a part of the Google Services System Security Plan maintained by the FedRAMP Program Management Office, and is available to government customers upon request. Customer may not use any Services to store or process classified information data.

37. Access Approval. Use of Access Approval may increase response times for TSS, and Customer will be responsible for any disruption or loss as a result of Customer denying or delaying approval via Access Approval. The SLAs do not apply to any Service disruption impacted by Customer’s use of Access Approval.

38. Security Command Center.

a. *Data Processing*. In order to protect your assets against new and evolving threats, Security Command Center analyzes data related to misconfigured assets, indicators of compromise in logs, and attack vectors. This activity may include processing to improve service models, identifying recommendations to harden customer environments, collecting metrics to evaluate the effectiveness and quality of services, and conducting experiments to optimize the user experience.

b. *Cryptomining Protection Program*. Customer’s use of Security Command Center Premium is subject to the terms of the Security Command Center Cryptomining Protection Program (“Cryptomining Protection Program”) (<https://cloud.google.com/security-command-center/cryptomining-protection-program?hl=en>). Google reserves the right to update or discontinue the Cryptomining Protection Program upon 30 days notice.

c. *Security Command Center Enterprise*. The SecOps Service Specific Terms (<https://cloud.google.com/terms/secops/service-terms?hl=en>) (and, other than this subsection, not these Google Cloud Platform Service Specific Terms) apply to your use of the Google Security Operations and Mandiant Attack Surface Management components (as each is described in the SecOps Services Summary (<https://cloud.google.com/terms/secops/services?hl=en>)) of Security Command Center Enterprise.

39. Cloud Identity Services. The following terms apply only to the Cloud Identity Services provided under this Agreement:

- a. *Use of Google Workspace Components.* Customer's use of the Google Workspace Components is subject to any applicable provisions of the then-current Google Workspace Service Specific Terms at <https://workspace.google.com/intl/en/terms/service-terms/>, which provisions are incorporated by reference into this Agreement.
- b. *Additional Products.* Google makes optional Additional Products available to Customer and Customer End Users through the Cloud Identity Services. Customer's use of Additional Products is subject to the Additional Product Terms.
- c. *Governing agreement.* Customer's use of Cloud Identity Services under the Account, will be governed by: (i) Customer's Google Workspace agreement; (ii) this Agreement; or (iii) the terms at <https://cloud.google.com/terms/identity>, if and as applicable, depending on which is in effect. This Section will survive expiry or termination of this Agreement.

d. *Definitions.*

"Additional Products" means products, services and applications that are not part of the Services but that 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.

"Google Workspace Components" has the meaning given in the then-current services summary for Cloud Identity Services at <https://cloud.google.com/terms/identity/user-features>.

"Google Workspace" means the then-current services described at https://workspace.google.com/terms/user_features.html

40. Firebase Authentication and Identity Platform.

a. *Phone Authentication.* Google temporarily stores phone numbers provided for authentication to improve spam and abuse prevention across Google services. Phone numbers are not logically isolated for a given customer's end users. Customer should obtain appropriate end-user consent before using the Firebase Authentication or Identity Platform phone number sign-in service.

b. *Other Authentication Services.* Use of Google Sign-In for authentication is subject to Google's API Services: User Data Policy (<https://developers.google.com/terms/api-services-user-data-policy>). Google is not responsible for any third-party sign-in service used with Firebase Authentication or Identity Platform.

c. *reCAPTCHA Notice Requirement.* Customer agrees to explicitly inform Customer End Users of phone authentication features that their use of reCAPTCHA is subject to the Google Privacy Policy (<https://policies.google.com/privacy>) and Terms of Use (<https://policies.google.com/terms>). For users in the European Union, you and your Application(s) must comply with the EU User Consent Policy (<https://www.google.com/about/company/user-consent-policy/>). Google collects hardware and software information, such as device and application data, through reCAPTCHA only as necessary to provide, maintain, and improve the Service, and for general security purposes. Such information will not be used for any other purpose, such as personalized advertising by Google.

41. **reCAPTCHA Enterprise.**

- a. *Information.* Google processes information submitted via use of the Service only as necessary to provide and maintain the Service, and ensure that the Service's security, threat detection, protection, and response capabilities remain effective against evolving threats. Such information will not be used for any other purpose, such as personalized advertising by Google.
- b. *Terms.* Customer will inform applicable Customer's End Users that Customer has implemented reCAPTCHA Enterprise on its properties and that Customer's End Users' use of reCAPTCHA Enterprise is subject to the Privacy Policy (<https://policies.google.com/privacy>) and Terms of Use (<https://policies.google.com/terms>).
- c. *Use.* reCAPTCHA Enterprise may only be used to fight fraud and abuse on Customer's properties, and not for any other purposes, such as determining credit worthiness, employment eligibility, financial status, or insurability of a user.
- d. *Customer Privacy Policy.* Customer will provide and adhere to a privacy policy for its API client that clearly and accurately describes to applicable Customer End Users what user information Customer collects and how Customer uses and shares such information with Google and third parties. Customer will be responsible for providing any necessary notices or consents for the collection and sharing of this data with Google. Customer and its API client(s) will comply with the EU User Consent Policy (<https://www.google.com/about/company/user-consent-policy/>).

42. **Web Risk.**

- a. *Attribution.* Customer may display a warning about unsafe web resources for a particular site based on verification against Google's list of unsafe sites provided that (i) the applicable Customer Application has received from Google an updated list (via the applicable API method) before the expiration time provided by the applicable API response or within 30 minutes if no expiration time is specified; and (ii) Customer provides attribution and conspicuous notice that the reliability and accuracy of the protection cannot be guaranteed using language similar to the "Advisory Notice" subsection below.
- b. *Advisory Notice.* Google works to provide the most accurate and up-to-date information about unsafe web resources, but cannot guarantee that its information is comprehensive and error-free: some risky sites may not be identified, and some safe sites may be identified in error.
- c. *Brand Protection, Evaluate and Submission APIs.* Google uses URLs and associated data submitted through the Brand Protection product, Evaluate API or Submission API ("Submitted URLs, Content and Metadata") and corresponding maliciousness scores to provide, maintain, protect and improve Google's products and services, including Google's list of unsafe web resources. Google may also share Submitted URLs, Content and Metadata with third parties, including other Google customers and users. Submitted URLs are not Customer Confidential Information or Customer Data.

43. **Chrome Enterprise Premium.**

- a. *Chrome Enterprise Core.* In order to use Chrome Enterprise Premium Threat and Data Protection Services:



- (i) Customer agrees to the Chrome Enterprise Core Agreement at <https://chromeenterprise.google/terms/chrome-enterprise-core/>; and
 - (ii) Customer acknowledges and agrees that Customer must enable “Chrome Enterprise Connectors” in the Chrome Browser section of the Admin Console.
- b. *Threats*. When Chrome Enterprise Premium checks for malware, unsafe web pages, or other unsafe files (“Threats”), the URL or a file hash and the result of the analysis are temporarily stored in a Google global cache for performance-related purposes. Customer acknowledges and agrees that Customer URLs, content, metadata and file hashes that Chrome Enterprise Premium identifies as Threats are not Customer Confidential Information or Customer Data and Google may use such URLs, content, metadata and file hashes to provide, maintain, protect and improve Google's products and services, including Google's lists of Threats, including without limitation sharing the same with third parties, including other customers and users.
- c. *App Connector*. Customer agrees to install Software for App Connector in Customer's private data center or other non-Google cloud environments in accordance with the minimum specifications described in the Documentation. Customer authorizes Google to connect and maintain the Software in order to provide connectivity for the applications accessed by Customer via App Connector.

44. Certificate Manager. Customer authorizes Google Cloud to apply for and obtain publicly trusted SSL/TLS certificates from third-party or Google-managed certificate authorities for domains operated and controlled by Customer (“Customer Domains”) pursuant to the CA/Browser Forum Baseline Requirements or any applicable successor requirements (“Requirements”). Customer represents and warrants that it operates and controls the Customer Domains and will revoke the authorization from Google when Customer ceases to operate and control a Customer Domain. Google may revoke a certificate as required by the Requirements or for failure to comply with the AUP.

45. Audit Manager. Reports generated by Audit Manager support information gathering only and do not determine or attest to compliance with any compliance standard. Use of Audit Manager neither relieves Customer of nor substitutes for any of Customer's obligations to verify compliance; Customer remains responsible for separately verifying its compliance with applicable compliance standards.

Google Distributed Cloud

46. Google Distributed Cloud connected (formerly Google Distributed Cloud Edge). If you purchased Google Distributed Cloud connected prior to August 15, 2023, the terms available at <https://cloud.google.com/distributed-cloud/edge/service-terms> will apply.

Data Boundary by Partners

47. Data Boundary by Partners (formerly Sovereign Controls by Partners).

a. *Customer Responsibilities*. The Data Boundary by Partners solution applies only to the Supported Google Cloud Services listed at <https://cloud.google.com/terms/in-scope-sovereign-cloud> (“Supported Google Cloud

Services”). The Party using the Data Boundary Partner's solution, whether Customer or a customer of the Data Boundary Partner or other Reseller or Partner, is responsible for: (i) receiving the Data Boundary Partner's services, including external key management services (“EKM”), from a Data Boundary Partner listed at <https://cloud.google.com/terms/in-scope-sovereign-cloud>, and (ii) maintaining separate terms directly with the Data Boundary Partner governing the use of that Data Boundary Partner's services.

b. *Partner Access.* To the extent applicable, Customer authorizes (and will ensure, if applicable, it has all relevant approvals to allow) Google to share, with the relevant Data Boundary Partner, TSS case details and Customer's contact information, metadata, log data, billing information, and configuration data from the Services used in the environment applicable to the Data Boundary by Partners solution, or that of Customer's applicable end customer. Google is not responsible for a Data Boundary Partner's handling of such data.

c. *Key Access Justifications.* Google will transmit an accurate justification to the EKM for each request to obtain key access to decrypt Customer Data for supported, generally-available Services, pursuant to terms agreed between the Data Boundary Partner and Google (if applicable). Once the EKM receives a justification, they are responsible for determining whether to grant Google the requested key access. Google is not responsible if the operation or functionality of the Services is impacted because Google cannot obtain a key access needed for such operation or functionality.

d. *Security Controls.* Data location controls made available by Google for the Data Boundary by Partners solution will be the same as the controls Google makes available for Assured Workloads, as described in the Assured Workloads Service Specific Terms.

Databases

48. **AlloyDB Omni.** Users of the free AlloyDB Omni Developer Edition and their Software Users (as defined in the General Service Terms) may use the Alloy DB Omni Software only for the purposes of developing, testing, prototyping, and demonstrating software programs (in any environment). Such users and Software Users may not use the AlloyDB Omni Software for any data processing, business, commercial, or production purposes.

Premium Software

49. Telecom Subscriber Insights.

a. *Updates.* If Google makes available to Customer an update to the Telecom Subscriber Insights Software and Customer does not download the update within 30 days of notification of its availability, Google will automatically push the update to Customer's Project(s) that use Telecom Subscriber Insights.

b. *Additional Restrictions.* Customer will not (either directly or via third parties) (i) use Telecom Subscriber Insights or any of its components to create, train, or improve (directly or indirectly) any similar or competing system, product or service; or (ii) use output data from Telecom Subscriber Insights for the purpose of creating, training, or improving (directly or indirectly) any similar or competing system, product or service.

Free Evaluation Services

50. Free Evaluation Services.

a. Definitions.

"Free Evaluation Services" means (a) presales, evaluation, or proof-of-concept services; and (b) ad-hoc technical assistance (brief technical assistance to address immediate, isolated technical inquiries or minor operational issues) related to Google Cloud products, in each case provided to Customer free of charge by Google Personnel. Free Evaluation Services do not include work that falls under any agreement governing (i) implementation services or deliverables, (ii) ongoing, paid technical support services, or (iii) any similar scoped or on-going professional technical or consulting services by Google Personnel.

"Free Model" means a version of an artificial intelligence or machine learning model trained, adapted, or fine-tuned by Google Personnel as part of the Free Evaluation Services using Customer Data.

"Google Personnel" means Google's and its Affiliates' employees, agents, and subcontractors.

"Materials" means tools, code, algorithms, models, written documentation, and other technology provided to Customer by Google Personnel as part of the Free Evaluation Services.

b. *Scope.* Google will provide Free Evaluation Services in accordance with this Section. Free Evaluation Services may be provided without an Order Form. Free Evaluation Services are only intended to enable Customer to receive help, recommendations, learnings, and advice from Google Personnel to evaluate, demo, and learn how Customer can use Google Cloud products and services to meet its business use cases.

c. *Terms.* Free Evaluation Services are "Pre-GA Offerings" and will be subject to the Pre-GA Offerings Terms in the SSTs and any additional terms described in this Section (Free Evaluation Services). In addition to the terms of the Agreement excluded for Pre-GA Offerings, any terms specific to the function of the Services or Software, and not appropriate or relevant for Free Evaluation Services, such as provision of an Account or a Status Dashboard, location of Data Centers, or information about Significant Developments, do not apply to Free Evaluation Services. In addition, notwithstanding anything to the contrary in the Agreement, Google has no obligation to implement tools and measures designed to prevent the introduction of Viruses into Materials. (Customer may use tools and measures available as part of the Services to assess Materials for Viruses in Customer's Account.) To the extent permitted by applicable law, Google may assign a new subcontractor or subprocessor to provide Free Evaluation Services immediately upon written notice to Customer.

d. *Materials.* While Materials may be provided to Customer by Google, Free Evaluation Services do not create deliverables or new Intellectual Property for Customer. Google retains all Intellectual Property Rights in Materials, except to the extent Materials contain Customer Data owned or licensed by Customer (a) before the start date of the Evaluation Services or (b) independent of the Evaluation Services. Customer may use Materials for its internal business purposes only. Customer agrees and acknowledges that open source code may be included in



Materials. Nothing in this Section (Free Evaluation Services) grants any right for Customer to use any materials, products, or services that are otherwise made available to Google customers under a separate license or agreement.

e. Customer Obligations.

(i) *Non-Production Environment.* Customer will only provide Google Personnel with access to Customer Data for Free Evaluation Services in a non-production Google Cloud Platform environment managed by Customer. Google will only access, use, and otherwise process Customer Data to provide the Free Evaluation Services.

(ii) *Customer Personal Data.* Customer will not provide Google Personnel with access to Customer Personal Data (as defined in the Cloud Data Processing Addendum) to receive Free Evaluation Services unless the parties have defined the scope and purpose of Google's access to such Customer Personal Data in a separate agreement. If Google discovers that Customer has provided Google Personnel with access to Customer Personal Data, Google will suspend performing Free Evaluation Services until Customer deletes such Customer Personal Data. If the Parties agree that Google will access Customer Personal Data in a separate agreement, then (a) the Cloud Data Processing Addendum will apply, but only with respect to Customer Personal Data, and (b) Free Evaluation Services will be treated as Implementation Services in the Cloud Data Processing Addendum (with the exception of Google's Compliance Certification obligations for Implementation Services).

f. *AI Services.* If Free Evaluation Services involve helping Customer to evaluate Google Cloud's artificial intelligence or machine learning products and services:

(i) Customer will have sole access to any Free Model; Google will not use any Free Model for its own purposes or provide a Free Model to any other Google customer.

(ii) Data or content generated by a Free Model will be treated as Generated Output, even if not generated by a Generative AI Service.

(iii) Customer's use of a Free Model provided to Customer by Google will be subject to the Generative AI Service Disclaimer, the AUP, the Prohibited Use Policy located at <https://policies.google.com/terms/generative-ai/use-policy>, and the "Restrictions" or "Use Restrictions" sections in the Agreement and AI/ML Services Section of the Service Specific Terms, in each case regardless of whether such Free Model includes a Generative AI Service.

Third-Party Terms

1. Red Hat Enterprise Linux.

Customer's use of the Red Hat Enterprise Linux product, provided by Google in conjunction with Compute Engine, is subject to the terms and conditions stated at https://www.redhat.com/licenses/cloud_cssa/.

2. Microsoft Products.

Customer's use of the Microsoft products, which may include associated media, printed materials, and "online" or electronic documentation (individually and collectively, "Microsoft Products"), provided by Google in conjunction with any applicable Service(s) is subject to the terms and conditions stated at <https://cloud.google.com/terms/service-terms/microsoft>.



3. **NVIDIA Drivers.**

The NVIDIA software components used in conjunction with the Services are subject to the terms and conditions stated at

<https://cloud.google.com/terms/service-terms/nvidia>. Notwithstanding the preceding sentence, the NVIDIA Linux GPU kernel modules identified at <https://github.com/NVIDIA/open-gpu-kernel-modules> will be made available under, and subject to, the open source terms included on that page.

In addition, the following NVIDIA software components may be used solely with the Services for compute and offline graphics purposes: GRID, Tesla Driver, Cuda Toolkit, cuDNN, TensorRT, NVENC, NVCUVID, NVML, and nvidia-aml.

4. **Oracle JDBC Driver in Looker (Google Cloud core) only.**

The Oracle JDBC software components used in conjunction with the Looker (Google Cloud core) service are subject to the terms and conditions stated at

<https://cloud.google.com/terms/looker/legal/customers/service-terms/oracle>.

5. **Ubuntu Pro (Canonical).**

Customer's use of Ubuntu Pro (a product of Canonical Group Limited), provided by Google in conjunction with Compute Engine, is subject to the terms and conditions stated at <https://ubuntu.com/legal/ubuntu-pro-service-terms>.

6. **Squarespace Domains.**

Customer's use of Squarespace Domains purchased through Google Cloud Platform is subject to the terms and conditions stated at Squarespace's Terms of Service (<https://www.squarespace.com/terms-of-service>) (excluding the section entitled "Paid Services and Fees", as all payments will be in accordance with the Agreement), Squarespace's Domain Registration Agreement (<https://www.squarespace.com/domain-registration-agreement>), and Squarespace's Privacy Policy (<https://www.squarespace.com/privacy>).

Pricing and Billing Terms

1. **Committed Units.**

a. *Selection and Commitment.* If Customer purchases Committed Units, then notwithstanding the payment terms in the Agreement, Customer will pay the Fees for those Committed Units during the Committed Unit Term selected by Customer, whether or not they are used, as stated at the Fees URL for the applicable SKU. The Fees for some Committed Units may be fixed for the duration of the Committed Unit Term to the price in effect at the beginning of that Committed Unit Term, as described in the applicable Documentation.

b. *Renewal.* Unless otherwise stated in the Admin Console or other documentation, at the end of each Committed Unit Term, the Committed Unit selection will automatically renew for the same Committed Unit Term at the same quantity until Customer selects in the Admin Console to stop renewing or either party notifies the other party in writing to cancel the renewal.

c. *Cancellation and Expiration.* If Google serves notice to non-renew the Agreement, terminates the Agreement (other than for Customer's material breach), or



discontinues providing the Services applicable to the Committed Units, Google will refund Customer any unused prepaid Fees following the expiration or termination of the Agreement, or discontinuance of the relevant Services, as applicable. Any use of the Services after cancellation or expiration of the Committed Units will be billed at standard Fee rates.

d. *No Resell or Transfer.* Unless Google agrees otherwise, Customer may not resell or transfer Committed Units. Further, unless Google agrees otherwise in writing, Partners may not transfer or share Committed Units between multiple customers.

2. **Currency Conversion.**

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

3. **SAP S/4HANA.**

If Customer is purchasing the SAP S/4HANA offering from SAP and has made financial commitments for expenditure on Google Cloud Platform Services in an addendum to the Agreement, then Google agrees to apply the dollar amount (net of any credits, discounts and Taxes) of Google Cloud Platform infrastructure services consumed by SAP in delivering SAP S/4HANA to Customer under the SAP S/4HANA Cloud Contract (the “SAP Allocation”) towards Customer’s then-current commitment. If Customer has multiple commitments, then the SAP Allocation will be applied towards the commitment that was most recently entered into with Google. Customer acknowledges that SAP will provide Google with the information necessary for Google to obtain the accurate volume of Google Cloud Platform infrastructure services consumed by SAP under the framework of Customer’s SAP S/4HANA Cloud Contract, and agrees that Google may use this information to determine the monetary amount to be counted towards Customer’s commitment. For the purposes of this subsection:

“SAP” means SAP SE, a company registered in Germany, or its Affiliate, as applicable.

“SAP S/4HANA Cloud Contract” means the separate contract between Customer and SAP (entitled “RISE with SAP S/4HANA Cloud Private Edition-SAP RISE Order Form”) under which the SAP S/4HANA Cloud (private edition) is made available by SAP to Customer.

This Section (SAP S/4HANA) does not apply to any customer accessing Google Cloud Platform Services as a customer of an unaffiliated Google Cloud Platform reseller.

4. **Additional Definitions.**

“*Committed Units*” means a non-cancellable (a) specified quantity of the Services (e.g. Compute Engine virtual machine instances), which may include a specified machine type, region, zone, query capacity, and period of time to use; (b) specified amount of credits to be purchased for expenditure on specified Services during a specified time period; or (c) a specified quantity of the Services offered on a subscription basis during a specified time period.

“*Committed Unit Term*” means the period of time during which Customer is obligated to pay for the Committed Units.

“*Fees URL*” means <https://cloud.google.com/skus>.



“*Order Form*” means an order form executed by Customer and Google or an order placed by Customer via a Google website, in either case specifying the Services Google will provide to Customer.

5. Price Change Rationale.

To the extent Google has a right to modify Prices under the Agreement, it may have various reasons for doing so, including (for example, and without limitation): (a) changes in Google's underlying costs for developing, providing, maintaining, and/or selling the Services, such as costs related to hardware, software licenses, energy, labor, and data center infrastructure; (b) enhancements, modifications, or changes to the nature, features, or functionality of the Services, including the introduction of new services or capabilities; (c) prevailing market conditions, including competitive pressures, inflation, deflation, or currency exchange rate fluctuations; (d) changes in applicable laws, regulations, taxes, or other compliance requirements that impact the cost or manner of delivering the Services; (e) the evolution of technology and industry standards affecting the Services; and (f) changes to costs payable by Google to third parties.

Partner-Specific Terms

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

a. A “Partner Customer” will mean an entity to whom Partner resells or supplies the Services under the Agreement.

b. Any references to a Customer Application means an Application.

c. The subsection of these Services Specific Terms under “Generative AI Services” titled “Restrictions” will be amended to state:

The restrictions contained in subsections (d) and (e) above are deemed to be additional restrictions in the “Use Restrictions” section under the applicable Agreement’s Google Cloud Platform Product Schedule.

d. The definition of a Customer Adapter Model will mean:

“Customer Adapter Model” means an adapter model that Partner or a Partner Customer creates using its Partner Data with an AI/ML Service.

e. The definition of a Customer Model will mean:

“Customer Model” means (i) a model that Partner or a Partner Customer creates without using a Google Pre-Trained Model or (ii) a model owned by Partner, a Partner Customer, or a third party that Partner or a Partner Customer uploads, fine-tunes, or deploys in AI/ML Services. Customer Models do not include Customer Adapter Models.

f. The definition of a Fine-Tuned Google Model will mean:

“Fine-Tuned Google Model” means an uptrained model that Partner or a Partner Customer creates by using an AI/ML Service to retrain or fine-tune a Google Pre-Trained Model using Partner Data.

g. The Partner or Partner Customer (as applicable) that creates a Fine-Tuned Google Model will have sole access to use that Fine-Tuned Google Model.

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

a. *Sublicensing.*

(i) Partner may sublicense Software, but only to its Customers who are obtaining the Software from Partner (“Authorized Sublicensees”).

(ii) Partner may not grant any Authorized Sublicensee the right to further sublicense any Software.

b. *Provision Limitations.* Unless Google has provided specific written instructions otherwise, Partner may not directly provide the Software to any third party (including any Authorized Sublicensee) and will instruct Authorized Sublicensees to directly download the Software from a URL or other repository provided by Google.

3. SAP S/4HANA (Partner).

If a Partner Customer is purchasing the SAP S/4HANA offering from SAP and Partner has made financial commitments for expenditure on Google Cloud Platform Services with respect to that Partner Customer in an addendum to the Agreement, then Google agrees to apply the dollar amount (net of any credits, discounts, and Taxes) of Google Cloud Platform infrastructure services consumed by SAP in delivering SAP S/4HANA to Partner Customer under the SAP S/4HANA Cloud Contract (the “SAP Allocation”) towards Partner’s then-current commitment with respect to that Partner Customer. If Partner has multiple commitments with respect to a Partner Customer, then the SAP Allocation will be applied towards the commitment that was most recently entered into with Google. Partner acknowledges that SAP will provide Google with the information necessary for Google to obtain the accurate volume of Google Cloud Platform infrastructure services consumed by SAP under the framework of Customer’s SAP S/4HANA Cloud Contract, and agrees that Google may use this information to determine the monetary amount to be counted towards Partner’s applicable commitment. Partner will obtain any consents from Partner Customer necessary to allow for the provision and use of information described in the preceding sentence. Notwithstanding the foregoing, if a Partner Customer has a separate financial commitment directly with Google to which the SAP Allocation is being applied, then this Section (SAP S/4HANA (Partner)) will not apply to Partner with respect to that Partner Customer.

For the purposes of this subsection:

“SAP” means SAP SE, a company registered in Germany, or its Affiliate, as applicable.

“SAP S/4HANA Cloud Contract” means the separate contract between Partner Customer and SAP (entitled “RISE with SAP S/4HANA Cloud Private Edition-SAP RISE Order Form”) under which the SAP S/4HANA Cloud (private edition) is made available by SAP to Partner Customer.



SecOps Service Specific Terms

The Service Specific Terms specific to one or more SecOps Services or Software can be found at: <https://cloud.google.com/terms/secops/service-terms>, which are incorporated into these Service Specific Terms. The SecOps Service Specific Terms (and other than this section, not these GCP Service Specific Terms) apply to Customer's use of SecOps Services and Software (as each is described in the SecOps Services Summary (<https://cloud.google.com/terms/secops/services?hl=en>)).

Previous versions (*Last modified December 22, 2025*)

November 20, 2025 October 16, 2025 October 9, 2025 October 6, 2025 September 25, 2025 September 18, 2025 September 9, 2025 August 28, 2025 August 18, 2025 July 1, 2025 June 9, 2025 May 15, 2025 April 8, 2025 February 6, 2025 December 16, 2024 November 11, 2024 October 24, 2024 October 22, 2024 September 30, 2024 September 9, 2024 July 18, 2024 July 15, 2024 June 27, 2024 June 6, 2024 May 29, 2024 May 14, 2024 April 24, 2024 April 9, 2024 March 12, 2024 March 7, 2024 February 29, 2024 February 21, 2024 January 15, 2024 December 20, 2023 December 5, 2023 November 20, 2023 October 24, 2023 October 12, 2023 October 11, 2023 September 25, 2023 August 28, 2023 August 14, 2023 June 29, 2023 June 5, 2023 May 24, 2023 May 8, 2023 May 2, 2023 April 27, 2023 April 11, 2023 April 3, 2023 March 30, 2023 March 27, 2023 February 9, 2023 December 19, 2022 November 7, 2022 October 27, 2022 October 11, 2022 October 3, 2022 September 20, 2022 August 31, 2022 August 22, 2022 August 1, 2022 July 6, 2022 June 28, 2022 June 16, 2022 April 25, 2022 April 12, 2022 April 4, 2022 March 31, 2022 March 21, 2022 December 15, 2021 November 30, 2021 October 18, 2021 September 30, 2021 August 24, 2021 July 20, 2021 June 22, 2021 June 3, 2021 May 18, 2021 April 30, 2021 January 26, 2021 January 19, 2021 January 5, 2021 December 8, 2020 November 2, 2020 October 6, 2020 September 1, 2020 August 19, 2020 August 7, 2020 July 13, 2020 June 30, 2020 June 10, 2020 April 29, 2020 April 27, 2020 April 22, 2020 April 15, 2020 March 26, 2020 March 11, 2020 January 13, 2020 December 3, 2019 November 12, 2019 November 4, 2019 October 30, 2019 October 1, 2019 July 1, 2019 June 17, 2019 May 31, 2019 April 9, 2019 March 27, 2019 January 17, 2019 December 13, 2018 October 19, 2018 September 28, 2018 August 29, 2018 August 15, 2018 August 2, 2018 July 24, 2018 July 6, 2018 June 25, 2018 June 5, 2018 May 8, 2018 April 24, 2018 April 18, 2018 April 4, 2018 March 21, 2018 March 14, 2018 February 16, 2018 November 30, 2017 November 13, 2017 October 31, 2017 October 10, 2017 October 5, 2017 September 25, 2017 September 13, 2017



SecOps Services Summary

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

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

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

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

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

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

Mandiant Solutions include:

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

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



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

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

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

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

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

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

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

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

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



SecOps Service Specific Terms

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

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

General Service Terms

1. Data

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

7. Generative AI Features.

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

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

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

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

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

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

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

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

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

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

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

by Reseller in accordance with the Reseller Agreement, subject to Section 9(e) (Reseller Technical Support);

vi. Customer acknowledges that access to the Services may be Suspended if at any time Reseller or Customer fails to maintain a billing account linked to Customer's Account;

vii. In the event of termination of the Agreement, Google will send Reseller (and not Customer) the final invoice (if applicable) for payment obligations related to Resold Services. Customer will notify (i) Reseller of any termination of the Agreement and (ii) Google of any termination of the Reseller Agreement;

viii. Any renewal(s) of the Resold Services and/or any Reseller Order will be as agreed between Customer and Reseller;

ix. If Reseller fails to pay an undisputed invoice for Resold Services to Google due to Customer's failure to pay Reseller, Google may Suspend Customer's access to the Services;

x. To the extent that any Customer Data is under Reseller's organizational resource, then notwithstanding anything to the contrary in this Agreement (including the Cloud Data Processing Addendum):

(A) the Cloud Data Processing Addendum will not apply with respect to the processing and security of such Customer Data;

(B) Google will only access, use, and otherwise process such Customer Data in accordance with the separate agreement between Google and Reseller (including its then-current terms describing data processing and security of "Partner Data" as defined by that agreement) and will not access, use, or process such Customer Data for any other purpose; and
(C) the consents and notices for which Customer is responsible under the section of this Agreement titled "Privacy" or "Consents" must also permit accessing, storing, and processing of Customer Data as described in subsection (B) above.

xi. Certain SecOps Services require linking to the Reseller's billing account in order to be billed by the Reseller. Customer acknowledges and agrees that, (A) if Google's agreement with the Reseller or Customer's Reseller Agreement is terminated or expires, then the Services will no longer be linked to the Reseller's billing account, and (B) unless any such Services used by Customer are linked to the Reseller's billing account, such Services will (x) not constitute Resold Services (and therefore not be subject to this Section 9 (Resold Customers)), and (y) be regarded as Services ordered directly from Google and accordingly, despite the terms of the Reseller Agreement (including the fees agreed between Customer and Reseller), Customer will be required to pay Fees to Google for such Services, in accordance with the terms of this Agreement. For inquiries about which SecOps Services must be linked, Customer should contact Reseller.

xii. "Cloud Data Processing Addendum," as it is used in this Agreement, means the then-current terms describing data processing and security obligations with respect to Customer Data that is (i) under Customer's (and not Reseller's) organizational resource or (ii) related to Mandiant Consulting Resold Services or Mandiant Managed Resold Services, as described at <https://cloud.google.com/terms/data-processing-addendum/>.

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



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

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

11. Additional Definitions.

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

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

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

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

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

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

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

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

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

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

“SecOps Services Locations Page” means

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

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

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



Service Terms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

2. Mandiant

a. Mandiant Solutions

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

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

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

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

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

ii. Security Content.

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

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

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

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

b. Mandiant Managed Services

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

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

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

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

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



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

c. Mandiant Consulting Services

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

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

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

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

vi. Intellectual Property.

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

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

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

vii. Warranties and Remedies.

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

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

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

viii. Indemnification.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

e. Training Services

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



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

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

f. Additional Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- i. Sublicense, distribute, publicly perform or display, or otherwise share or make accessible, directly or indirectly, any Platform Security Content or results from GTI, including without limitation, any Google API or interface, or portions thereof, to any third party.
- ii. Obtain or use any Platform Security Content except as specifically permitted, or use or attempt to use GTI to mine information in any way that could identify individual persons in their private capacity, attempt to access or misappropriate content contained in any Platform Security Content, or otherwise use GTI or Platform Security Content for any purpose other than to detect and prevent malware in a non-commercial personal or organizational capacity.
- iii. Publicly attribute the Platform Security Content that Customer receives through GTI to any Security Partner (including, but not limited to any antivirus vendors, URL scanning engines, file characterization tools, etc.) without the individual Security Partner’s express written permission.

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

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

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

e. Customer Submitted Content and Community Content Guidelines.

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

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

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

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

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

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

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

iii. *Requirements.* Customer will:

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

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

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

- B. *Public Facing Materials.*

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

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

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

Reports.

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

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

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

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

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

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

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

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

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

k. Additional Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

4. Security Customer Success Services.

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

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

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

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

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



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

Partner-Specific Terms

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

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

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

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

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



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



Google Cloud Platform Terms

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

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

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

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

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



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

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

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

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

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

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

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



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



Google Workspace Service-Specific Terms

Last modified: 13 October 2025

For translations of these Service-Specific Terms into other languages, please click here (https://workspace.google.com/intl/en_uk/terms/translations/).

Capitalised terms not defined in these Service-Specific Terms for Google Workspace (formerly known as G Suite) have the meaning stated in the Google Workspace Services Schedule to the Google Cloud Master Agreement, Google Workspace for Education Agreement or other applicable agreement governing the use of Google Workspace Services (in each case, the 'Agreement').

1. Data Regions.

1.1 Primary data storage. Subject to Section 1.2 (AppSheet primary data storage), if the Customer is using an In-Scope Edition of the Services, the Customer may select a Data Region to (a) process Located Data in use by the configured Service to the extent permitted by the Service and (b) store Located Data at rest, and Google will, in accordance with applicable law, process and store such Located Data accordingly ('Data Regions Policy').

1.2 AppSheet primary data storage. The Data Regions Policy applies to AppSheet (even if included in an In-Scope Edition of the Services) only where (a) the Customer uses AppSheet Enterprise Plus and (b) an End User has selected specific Located Data to store in the Data Region.

1.3 Limitation. For any Customer Data that is not covered by the Data Regions Policy, Google may store or process such data, as applicable, anywhere that Google or its Sub-processors maintain facilities, subject to the Cloud Data Processing Addendum.

1.4 Definitions.

'Located Data' means only the following primary data within Customer Data for the corresponding Service:

- (a) Gmail: Subject line and body of emails, senders and recipients of messages and attachments.
- (b) Google Calendar: Event titles and descriptions of events, dates, times, invitees, frequency, locations and attachments.



- (c) Google Chat: Messages (including regular and customer status messages), attachments and room names.
- (d) Google Classroom (data storage at-rest only): Class title, class announcements, class assignments and materials posted by educators, originality reports, class rosters of students and educators and student marks.
- (e) Google Docs, Google Sheets, Google Slides and Google Vids: File body texts, embedded images, drawings and associated End User-generated comments.
- (f) Google Drive: Original file content uploaded to Drive (including texts, embedded images, drawings and associated End User-generated comments).
- (g) Google Vault: Vault exports.
- (h) AppSheet: App definitions, data source configurations and access tokens, and Customer Data in AppSheet databases.
- (i) Google Forms (data storage at-rest only): Text, embedded images, responses and draft responses.
- (j) Google Keep (data storage at-rest only): Note text and titles, images, drawings and audio recordings.
- (k) Google Meet: Meet recordings (including chats in Google Drive), attendance reports, polling results, transcripts and questions.
- (l) Google Sites (data storage at-rest only): Text, embedded images, embedded site information and embedded HTML/CSS/JavaScripts.
- (m) Gemini in Workspace: User prompts and Generated Output.

'Data Region' means :

- (a) either the United States or Europe, except in relation to AppSheet; or
- (b) Europe, in relation to AppSheet.

'In-Scope Edition' means the following editions:

- (a) G Suite Business
- (b) Google Workspace Enterprise Plus



- (c) Google Workspace for Education Standard
- (d) Google Workspace for Education Plus

2. **Google Vault.** The following terms apply only to Google Vault:

2.1 Retention. Google will have no obligation to retain any archived Customer Data beyond the retention period specified by the Customer or the Order Term applicable to the relevant Google Vault licences, unless: (a) before the expiry of that retention period, the Customer extends the retention period or renews the relevant Order Term; (b) applicable legislation or legal process prevents Google from deleting the data; or (c) the data is subject to a legal hold imposed by the Customer.

3. **Google Workspace Essentials.** The following terms apply only to the Google Workspace Essentials and Google Workspace Essentials Starter edition(s), as indicated:

3.1 Termination for inactivity or convenience. If the Customer orders the Google Workspace Essentials Starter edition, Google reserves the right to terminate the provision of Google Workspace Essentials Starter edition:

- (a) upon 30 days' notice to the Customer if, for any period of 60 consecutive days preceding the date of the notice, there has been no access to the Admin console or use of the Services by the Customer or any of its End Users; or
- (b) for convenience upon 90 days' notice to the Customer.

3.2 Technical Support Services. TSS is not available for Google Workspace Essentials Starter edition.

4. **Cloud Search.** The following terms apply only to Cloud Search:

4.1 Third-party data sources. The Customer's use of third-party data sources in connection with Cloud Search Platform is subject to and governed by the terms and conditions agreed between the Customer and the applicable provider of the data source. As between the parties, the Customer bears sole responsibility for such Terms and Conditions, including for ensuring that they allow Google to access and use the relevant data sources when providing Cloud Search Platform.

5. **Cloud Identity Services.** The following terms apply only to Cloud Identity Services provided under the Agreement:

5.1 Governing Agreement. If, in addition to the Agreement, the Customer's use of Cloud Identity Services under the Account is subject to a Google Cloud Platform agreement ('GCP Agreement') and/or the terms at <https://cloud.google.com/terms/identity> ('Cloud Identity TOS'), then the documents will control in the following order (of decreasing precedence): (a) the Agreement; (b) the GCP Agreement; or (c) the Cloud Identity TOS. This section will survive expiry or termination of the Agreement.

5.2 Additional definitions.

'Google Cloud Platform' means the then-current services described at <https://cloud.google.com/terms/services>.

6. Pre-General Availability Offerings Terms. Google may make available to the Customer, via a Test Application (as defined below), Pre-General Availability Google Workspace features, services or software that are identified as 'Early Access', 'Alpha', 'Beta', 'Preview', 'Experimental' or a similar designation in the Google Workspace Services Summary, related documentation or materials, or a Test Application (collectively, 'Pre-GA Offerings'). While Pre-GA Offerings are not Services, the Customer's use of Pre-GA Offerings is subject to the terms of the Agreement applicable to Services, as amended by this Section 6.

6.1 Access to and use of Pre-GA Offerings.

(a) Access to Pre-GA Offerings. Unless otherwise specified by Google, if the Customer wants to use a Pre-GA Offering, the Customer must apply to be a test user by submitting the application available via the Admin console or otherwise from Google ('Test Application(s)'). If accepted as a test user (based on Google's then-current domain-level requirements for test users), Google will make that Pre-GA Offering available for use by the Customer subject to the terms of this Section 6. Additional terms ('Specific Test Terms') may apply to that Pre-GA Offering and, if applicable, will be provided by Google via the Test Application or otherwise in writing before any use by the Customer. The Test Application and any Specific Test Terms are incorporated into this Section 6.

(b) Use of Customer Test Data. Subject to Sections 6(d) (Use Restriction for Government Customers) and 6(e) (Use Restriction for Protected Health Information) below, Google may use, and the Customer will (including by collecting or providing any required consents or notices) ensure that Google may use any Customer Data (including Customer Personal Data) submitted, stored, sent or received via any Pre-GA Offerings by the Customer or its End Users ('Customer Test Data') to provide, test, analyse, develop and improve those Pre-GA Offerings and any Google products and services used with them without any restriction or obligation to the Customer, any End User or any third party, other than as stated in the Agreement's confidentiality provisions and below.

If the Customer has accepted or the parties have otherwise agreed to Google's then-current terms describing data protection and processing obligations with respect to the Customer Data as

stated at

<https://cloud.google.com/terms/data-processing-addendum> (the 'Cloud Data Processing Addendum' or 'CDPA'), the CDPA will apply to Pre-GA Offerings as 'Services' for the purposes of the CDPA and, for clarity, this Section 6 will form part of the 'Agreement' referred to in Section 5.2 (Compliance with the Customer's instructions) of the CDPA, subject to the following amendments:

- (i) the Customer acknowledges that, for the purposes of Section 6.1 (Deletion by the Customer) of the CDPA and to the extent permitted by applicable law, the functionality of the Pre-GA Offerings may not allow the deletion of Customer Test Data during the period in which the Customer is permitted to use the Pre-GA Offering ('Pre-GA Term'), but that Customer Test Data will be deleted upon expiry of the Term in accordance with Section 6.2 (Return or deletion when Term ends) of the CDPA;
- (ii) Unless stated otherwise in Specific Test Terms: (A) information about Sub-processors (as defined in the CDPA) engaged in relation to Pre-GA Offerings, including their functions and locations, will be made available in writing by Google upon request from the Customer; and (B) Google will inform the Customer of the engagement during the Pre-GA Term of any new third-party Sub-processor engaged by Google in relation to Pre-GA Offerings (including the name and location of the Sub-processor and its activities) by sending an email to the notification email address before the Sub-processor starts processing any Customer Test Data. The Customer may, as its sole and exclusive remedy if the Customer objects to the Sub-processor, cease using the applicable Pre-GA Offering.
- (c) No data location or access transparency. Customer Test Data processed under this Section 6 will not be subject to any data location requirements (as described in Section 1 (Data Regions) of these Service-Specific Terms) or access transparency

requirements (as described at

<https://support.google.com/a/answer/9230474>).

(d) Use restriction for government customers. Unless authorised in writing by Google, the following customers may use only test or experimental data with Pre-GA Offerings and are prohibited from using any 'live' or production data in connection with Pre-GA Offerings: US or other government customers, including federal, national, state, provincial or local government or regulatory entities or agencies, but excluding customers that are primarily educational institutions.

(e) Use restriction for Protected Health Information. The Customer may not use Pre-GA Offerings to process Protected Health Information as defined in the HIPAA.

6.2 Change, suspension or discontinuance. Pre-GA Offerings (including any of their features) may be changed, suspended or discontinued at any time without prior notice to the Customer.

6.3 Disclaimer. **PRE-GA OFFERINGS ARE PROVIDED 'AS IS', WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS OF ANY KIND, AND ARE NOT COVERED BY ANY SLA OR GOOGLE INDEMNITY. Except as otherwise indicated in Specific Test Terms for a given Pre-GA Offering, Pre-GA Offerings are not covered by TSS.**

6.4 Liability. Google will not be liable for any amounts in excess of the lesser of (a) the limitation on the amount of liability stated in the Agreement or (b) \$25,000. Nothing in the preceding sentence will affect exclusions from any limitation of liability in the Agreement with respect to the following: (1) death or personal injury resulting from negligence; (2) fraud or fraudulent misrepresentation; (3) infringement of the other party's intellectual property rights; or (4) matters for which liability cannot be excluded or limited under applicable law.

6.5 Termination. Google may terminate the Customer's use of a Pre-GA Offering at any time with written notice to the Customer, for any reason, including to allow other customers to use that Pre-GA Offering.

7. **Verification using Domain Email Address.** The following additional terms apply only when a Domain Email Address (rather than a Domain Name) is verified to use the Services:

7.1 Inviting End Users. The Customer may invite other users with a domain email address to use the Services. If those users accept the Customer's invitation to use the Services, they will be considered the Customer's End Users under the Agreement.

7.2 Domain name verification.

(a) Assumption of control by Verifying Party. Any person or entity may verify

the Domain Name corresponding to the domain email address at any time (Verifying Party). The Verifying Party will take ownership and control of End User Accounts corresponding to the Domain Name and all associated data within such End User Accounts immediately after verifying the Domain Name. The Customer and all End Users will be notified when the Domain Name is verified.

(b) Administration after Domain Name verification. A Verifying Party will have certain permissions with respect to the Customer's account and all such End User accounts, as described in the documentation.

7.3 Data deletion. At any time before the Verifying Party takes ownership and control of the Domain Name and all associated End User accounts (including the Customer's account), the Customer or its End Users will be able to delete or export Customer Data and/or delete its End User account(s) in a manner consistent with the functionality of the Services. After the Verifying Party takes ownership and control of the Domain Name and all associated End User accounts (including the Customer's account), then, notwithstanding any term to the contrary in the Cloud Data Processing Addendum, the Customer or its End Users may not be able to delete End User account(s) or delete or export any Customer Data depending on the administration of the Services.

7.4 Data processing instruction. If the Customer takes no action to delete or export any Customer Data before the Verifying Party takes ownership and control of the Domain Name and all associated End User accounts (including the Customer's account), then, notwithstanding Section 6.2 (Return or deletion when Term ends) of the Cloud Data Processing Addendum, the Customer acknowledges that these Service-Specific Terms document the Customer's instructions to Google to: (a) retain after termination of the Agreement as described in Section 7.6 (Termination after domain verification) all Customer Data that has not been deleted by the Customer prior to such termination; and (b) make such retained Customer Data available to the Verifying Party.

7.5 Consent to administration. Where applicable, the Customer agrees to allow: (a) the Verifying Party to have the access and capabilities described in the Agreement; and (b) Google to provide the Verifying Party with the access and capabilities described in the Agreement.

7.6 Termination after domain verification. Where the Verifying Party is a third party, the Agreement will automatically terminate when the Verifying Party takes ownership and control of the Domain Name and all associated End User accounts (including the Customer's account). For clarity, this section does not affect any End User rights that the Verifying Party may grant under its (separate) Google Workspace agreement.

7.7 Services limitations. Some Services, features and functionality may not be available unless and until the Domain Name is verified.

8. Google Telephony Services. The following terms apply only to (i) Google Voice and (ii) the use of Google Meet to perform outbound dialling and accept inbound calls ('Google Meet Telephony'), as applicable (and for the purposes of this Section 8, Google Voice and Google Meet Telephony are collectively referred to as 'Google Telephony Services'). THESE TERMS CONTAIN IMPORTANT INFORMATION ABOUT EMERGENCY SERVICES LIMITATIONS. PLEASE READ CAREFULLY:

8.1 Google Telephony Services Parties and Agreement Structure.

(a) Google Telephony Services Provider. The applicable Google entity listed in the applicable Service and Telephony Provider list (such entity in each case, the 'Google Telephony Service Provider' or 'GTSP') will provide the applicable Google Telephony Services to the Customer.

(b) Google Telephony Agreement structure. Where the applicable GTSP is a Google Affiliate and not Google, then in relation to the applicable Google Telephony Services only, Google contracts on behalf of the GTSP (having been duly authorised as its agent) and accordingly:

(i) If the Customer chooses to order any Google Telephony Services in addition to the other Services ordered by the

Customer under the Agreement, this Section 8.1 together with the other terms of the Agreement (including the CDPA and all limitations of liability) will form a separate agreement (the 'Google Telephony Agreement') entered into by the applicable GTSP (via Google as its duly authorised agent) and the Customer with respect to such Google Telephony Services only, subject to the remaining terms of this Section 8.1.

(ii) The Google Telephony Agreement will take effect as of the effective date of the Customer's initial order of Google Telephony Services and, subject to earlier termination in accordance with its terms, will continue until the earliest to occur of (A) termination of the Google Telephony Agreement in accordance with its terms; or (B) termination or expiry of the Agreement. The Google Telephony Agreement will supersede the Agreement only with respect to the Google Telephony Services.

(iii) For the purposes of the Google Telephony Agreement, all references (excluding those in the Services Summary and this Section 8 of these Service-Specific Terms) to 'Agreement' are replaced with 'Google Telephony Agreement'; to the entity 'Google' are replaced with 'GTSP'; and to 'Services' or

'Core Services' are replaced with 'Google Telephony Services'.

(iv) The Customer may enforce rights and benefits under the Google Telephony Agreement against GTSP only, not Google, and will owe obligations under the Google Telephony Agreement (including obligations to pay all applicable fees) to GTSP only, not Google.

(v) Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between this Section 8.1 and any other term of the Google Telephony Agreement (including the 'Conflicting Terms' section of the Agreement and the 'Precedence' section of the CDPA), the terms of this Section 8.1 will prevail.

(vi) Either party may terminate the Google Telephony Agreement separately from the Agreement as set out in the 'Term and Termination' section of the Agreement. If the Customer terminates its use of Google Voice as described in Section 8.10 (Termination of Google Voice by the Customer), such termination will automatically terminate the Google Telephony Agreement.

(c) Regional Terms. The Regional Terms are incorporated into the Google Telephony Agreement and apply to the extent that an End User uses Google



Voice in a country described in the Regional Terms.

8.2 Provision of Google Telephony Services.

(a) Data use.

(i) Data collection and use. GTSP will collect and use Customer Data in accordance with the Google Telephony Services Privacy Disclosure provided at https://workspace.google.com/terms/service-terms/voice/privacy_disclosure.html.

(ii) Subscriber directory. GTSP will not provide the Customer's or its End Users' Google Voice numbers to directory services unless requested to do so by the Customer or otherwise required by law.

(b) Telephony Providers.

(i) Affiliate Providers. GTSP may use its Affiliates to provide Google Telephony Services as described in the Service and Telephony Provider list.

(ii) Non-Affiliate Telephony Providers. GTSP and its Affiliates use non-Google third-party subcontractors (Telephony Providers) to route inbound and outbound telephone calls, as applicable, via the public switched telephone network (PSTN). Telephony Providers and their locations are identified in the Service and Telephony Provider List. By using Google Telephony Services, the Customer instructs GTSP to engage, and to have its Affiliates engage, Telephony Providers to:

(1) route outbound and inbound telephone calls, as applicable; and

(2) process Customer Data as independent controllers in the countries in which they are located:

(A) to the minimum extent required for such routing; and

(B) in accordance with applicable laws (including European data protection laws and telecommunications regulations).

For clarity, Telephony Providers are not sub-processors (as defined in the CDPA).

8.3 Additional payment terms.

(a) Google Telephony Services invoices. Applicable Fees and other costs arising from the Customer's or End Users' use of Google Telephony Services are invoiced separately from other Google Workspace Services, and are subject to the payment terms of the Google Telephony Agreement.

(b) Calling rates. In addition to the Fees, the Customer will pay GTSP for calls based on usage, if applicable. These usage costs are calculated using the then-current applicable calling rates.

(c) Taxes. Notwithstanding anything to the contrary in the Google Telephony Agreement, the Customer will pay applicable Taxes regardless of any tax exemption certificates. Invoiced taxes may include taxes associated with an End User's use of Google Telephony Services where such taxes are levied by a taxing authority outside of the country in which the End User is using Google Telephony Services.

8.4 Google Voice requirements; GTSP disclaimer.

(a) Google Voice requirements. **This Section 8.4(a) applies only to Google Voice and NOT to Google Meet Telephony.** Use of Google Voice may require a separate broadband or mobile data connection and an End User device compatible with certain minimum technical requirements. Out-of-country or other roaming usage of Google Voice may incur higher costs to End Users from their mobile network operators.

(b) GTSP disclaimer. GTSP is not responsible for any disruption or failure of Google Telephony Services due to delays, outages or disruptions in: (i) the Customer's data connection; (ii) Telephony Providers' networks; or (iii) the operation of Customer or End User devices. Using Google Telephony Services on mobile devices may use End



Users' voice or data allowances purchased from their mobile network operators.

8.5 Google Voice capabilities. This Section 8.5 applies only to Google Voice and NOT to Google Meet Telephony.

(a) Number assignment and availability. Where Google Voice permits the assignment of phone numbers, the following will apply:

- (i) number activation may require collection by GTSP of information required by applicable telecommunications regulations, including the Customer's service address and tax ID;
- (ii) in some countries, the service address must match the area covered by the number to be assigned;
- (iii) number activation may not be instantaneous upon request; and
- (iv) inactive numbers may be removed from the Customer's account.

(b) Number porting. The Customer may port existing numbers from other service providers to Google Voice, to the extent that Google Voice offers number assignment, and may request that assigned phone numbers be released to another service provider, subject to Sections 8.5(b)(i) and (ii) below.

(i) Customer obligations. The Customer is responsible for (A) the accuracy of information provided to GTSP associated with a porting request; (B) fees associated with porting a number, including fees associated with remaining numbers and plans; and (C) any Fees owed to GTSP associated with a number up to when the number is ported successfully, to the extent permitted by applicable laws.

(ii) Service termination. GTSP may release any Google Voice number after termination or expiry of the applicable End User licence if the Customer does not port the number to another service provider prior to such termination or expiry.

(c) Caller ID. Google Voice allows the display of the Customer's Google Voice number on receiving devices where technically possible. End Users may suppress the display of the number permanently or on a call-by-call basis. For technical reasons, GTSP

may not be able to suppress Google Voice numbers in all cases, including calls to emergency numbers.

(d) Number blocking. Upon the Customer's request, GTSP will block or unblock the use of Google Voice to call specific numbers, number ranges or types of numbers (including value-added services) to the extent technically feasible.

(e) Call recording. Google Voice may allow End Users to record individual telephone conversations. The Customer agrees not to, and not to allow its End Users to, record telephone conversations without consent if such consent is required by applicable laws or regulations.

8.6 Google Telephony Services limitations. Google Telephony Services may not:

- (a) include operator-assisted dialling and calls to short codes (additional fees may apply for these calls);
- (b) support 'reverse' or 'reverse charge' calls; or
- (c) support calls or connections to certain numbers, including, as an example, premium rate numbers.

8.7 Google Voice use restriction. **This Section 8.7 applies only to Google Voice and NOT to Google Meet Telephony.** The Customer will not sub-assign numbers to, provide access to or otherwise enable use of Google Voice by individuals under the age of legal consent as determined by the applicable laws of the relevant jurisdiction. GTSP may suspend or permanently disable any accounts that are used by or provisioned to such individuals.

8.8 Emergency services. **Subsection 8.8(a) applies only to Google Meet Telephony and NOT to Google Voice. All other subsections ((b)–(f)) of Section 8.8 apply only to Google Voice and NOT to Google Meet Telephony.**

(a) One-way dialling. End Users using one-way dialling features of Google Meet Telephony will not be able to place or receive emergency services calls. The Customer is responsible for ensuring that End Users have access to an alternative means of dialling the emergency services.

(b) Two-way dialling. Dialling the emergency services is supported by Google Voice. IP-based telephony emergency dialling services have certain limitations and will function differently from traditional emergency dialling as described in the provisions below; additional country-specific limitations are described in the Regional Terms. The Customer hereby acknowledges and accepts the following with respect to calls made to emergency services:

- (i) Description of emergency dialling service. End Users of the two-way

dialling features of Google Voice are capable of calling and receiving calls from the emergency services free of charge. Emergency services vary depending on the End User's location. When an End User calls emergency services, GTSP will provide to emergency response operators the End User's phone number and address that the Customer has provided to Google (see Section 8.8(d) (Customer obligations) below). End Users may need to confirm their physical location and call-back number because the emergency operator may not have this information.

(ii) Limitations on emergency dialling service. The following limitations apply to the availability of the Google Voice emergency dialling service: (A) the service may not be available in the event of an Internet or power outage or disruption; (B) emergency calls may take longer to connect to the public safety answering point than traditional emergency services dialling, may produce a busy signal or may not connect; (C) emergency calls may connect correctly to the PSAP, but the End User's phone number or location may not automatically be transmitted and the emergency services operator may not be able to call back; (D) emergency calls made while roaming may be routed to the local PSAP associated with the End User's registered address (the Customer will advise End Users to use their native dialler while roaming); (E) deaf, hard of hearing or speech impaired End Users should call local emergency services directly using TTY or a telecommunications relay service, instead of 711 or a local equivalent; (F) if End Users have multiple devices associated with their account number (1) return calls from the PSAP may not ring each associated device and (2) the emergency operator may see a phone

number that is different from the End User's personal phone number; (G) if the End User has disabled incoming calls, the PSAP may not be able to call back; (H) if a call fails using Google Voice, End Users may be directed to complete emergency calls using the native dialler on their devices; and (I) emergency calling is not available through this calling service if (1) using the inbound-only Google Voice service or (2) calls are directed through the voice network of the user's mobile operator, when using the native dialler of the End User's device.

(c) Texting to emergency services. Texting the emergency services may not be supported by Google Voice. Any text-to-emergency-services feature made available through Google Voice may not be supported over a Wi-Fi network.

(d) Customer obligations. With respect to Section 8.8(b) (Two-way dialling), the Customer is responsible for the following: (i) ensuring that the address registered within Google Voice for each End User is the current physical address where the End User will use Google Voice (failure to provide current addresses may cause the wrong emergency response centre to be contacted and delay the emergency response to End Users); (ii) informing End Users that their physical addresses will be shared with Telephony Providers; (iii) informing End Users that they may need to provide their physical location and call-back number to the PSAP, once connected; (iv) ensuring that End Users have access to an alternative means of calling emergency services; and (v) informing End Users of the limitations of the emergency dialling services (the Customer may download and print a warning label to affix to all devices that may be used to access Google Voice at

support.google.com/voice/go/emergency-services).

(e) Emergency alerts. Emergency alerts may not be received via Google Voice if devices are set to Wi-Fi only mode, or mobile service is not available.

(f) Disclaimer of emergency services liability. To the fullest extent permitted by law, neither GTSP nor any of its Affiliates will have any liability under the Google Telephony Agreement (whether in contract, tort (including negligence) or otherwise) for damages of

any type (including direct and indirect damages) arising under or in connection with the use or attempted use of Google Voice to access emergency services, including but not limited to any inability to access such services, any delays in emergency service response, the conduct of emergency services response centres or operators, or any inaccuracy of information provided to emergency services by Telephony Providers or other third parties engaged by GTSP or its Affiliates to facilitate the provision of emergency services access.

8.9 Suspension. In addition to the suspension rights described in the Google Telephony Agreement, GTSP may block incoming and outgoing Google Telephony Services calls or messages if GTSP reasonably determines that the Customer or any End User has used Google Telephony Services to generate or facilitate bulk or automated messages, or unsolicited commercial messages.

8.10 Termination of Google Voice by the Customer. **This Section 8.10 applies only to Google Voice and NOT to Google Meet Telephony.** In addition to any other termination rights, the Customer may terminate its use of Google Voice at any time by providing written notice to GTSP. The Customer must cease use of Google Voice immediately upon termination.

8.11 Additional definitions.

If an offline document refers to 'Google Voice Service Provider' or 'GVSP', those references are deemed to be a 'Google Telephony Services Provider' or 'GTSP' as used in these Service-Specific Terms and the Google Telephony Agreement.

9. Google SIP Link.

9.1 Additional Google SIP Link Terms. The following terms apply to the Customer's use of Google SIP Link:

- (a) Porting phone numbers to the Customer's SIP Provider must be effectuated by the SIP Provider.
- (b) The Customer acknowledges and agrees that Google may place calls to the Customer to validate the Customer's trunk configuration or verify number ownership. The Customer consents to receiving any such calls, including from an automated system.
- (c) The Customer is responsible for ensuring that any calls to emergency services made by a Google SIP Link user will be routed via the SIP Provider. Furthermore, the Customer must make any updates to its location or address for the purposes of emergency services through the SIP Provider.
- (d) For clarity, SIP Providers are not Sub-processors (as defined in the Cloud Data Processing Addendum).

9.2 Additional definitions.

'SIP Provider' means the Customer's systems integrator, operator or other partner who provides telephone service to the Customer independent of Google Voice.

10. **Google Drive.** The following terms apply only to Drive:

10.1 Use of Google Drive for Content Distribution. Google Drive is not intended for use as a content distribution network. Google may restrict Google Drive usage and access if Google, in its reasonable discretion, determines that Google Drive is being used in violation of the AUP or for infringing, unlawful or bulk distribution of content including videos. Any Google Drive-hosted video that is shared publicly outside of the Customer's domain must comply with YouTube Community Guidelines (available at <https://www.youtube.com/howyoutubeworks/policies/community-guidelines/> or a successor URL).

11. **AppSheet.** The following terms apply only to AppSheet:

11.1 Agreement Application. The Agreement, including these Service-Specific Terms, will apply only to the Customer's use of AppSheet with respect to End Users who access AppSheet via their End User Accounts and will not apply with respect to any AppSheet plan purchased on <https://www.appsheet.com>.

11.2 Administration of AppSheet. If the Customer's AppSheet plan includes additional management controls (as described at <https://about.appsheet.com/pricing/>), additional controls for the management and administration of AppSheet will be available to specifically designated Administrators for AppSheet.

11.3 Payment Terms. The definition of 'Prices' is amended to mean the then-current applicable prices at <https://solutions.appsheet.com/pricing>, unless otherwise agreed in an addendum or Order Form.

11.4 Data Sources. The Customer's use of Data Sources in connection with the Services is subject to and governed by the terms and conditions agreed between the Customer and the applicable Data Source provider. As between the parties, the Customer bears sole responsibility for such terms and conditions, including for ensuring that they allow Google to access and use the relevant Data Sources for providing AppSheet.

11.5 AppSheet Software. If Google makes AppSheet Software (which may include third-party software) available to the Customer, Google grants the Customer a royalty-free (unless otherwise stated by Google), non-exclusive, non-transferable licence during the Term to reproduce and use that Software for the purposes of making a Customer Application available to End Users, and may impose additional licensing restrictions with notice to the Customer. Any export, re-export, transfer or use by the Customer of the AppSheet Software is subject to the Agreement (including the restrictions and compliance obligations it imposes with respect to use of the Services, all of which will apply to the AppSheet Software), and may also be subject to

third-party licence terms and requirements under Export Control Laws. As between the parties, Google retains all Intellectual Property Rights in the AppSheet Software. Each party represents and warrants that it will comply with all laws and regulations applicable to its provision or use of the AppSheet Software, as applicable. EXCEPT AS EXPRESSLY PROVIDED FOR IN THE AGREEMENT, THE APPSHEET SOFTWARE IS PROVIDED 'AS IS' WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS OF ANY KIND.

11.6 Non-paid Versions.

(a) Limitations. Non-paid versions of AppSheet are subject to limitations and are not eligible for TSS, and certain features of AppSheet may not be available for non-paid versions. Google's indemnification obligations do not apply to use of AppSheet under non-paid versions.

(b) Termination for inactivity. Google reserves the right to terminate the provision of a non-paid version of AppSheet for an End User upon 30 days' advance notice to the End User if for a period of 60 days (i) the End User has not accessed AppSheet or (ii) there has been no activity on any Customer Application of the End User.

11.7 Discontinuation of AppSheet. Google will notify the Customer at least 12 months before discontinuing the AppSheet (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Nothing in this Section 11.7 (Discontinuation of AppSheet) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden.

11.8 Technical Support.

(a) Amendments. The definition of 'Google Workspace Technical Support Services Guidelines' or 'TSS Guidelines' is amended to mean the then-current AppSheet support service guidelines at <https://www.appsheet.com/Home/TSSG>.

(b) Customer Applications. The Customer is responsible for the technical support of its Customer Applications.

11.9 Additional definitions.

AppSheet Software means any downloadable tools, software development kits or other such computer software provided by Google in connection with AppSheet and any updates that Google may make to such AppSheet Software from time to time.

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



Data Source means the Google or third-party data sources described at <https://www.appsheet.com/Home/StartWithData>.

12. Workspace Generative AI Services. The following terms apply only for Workspace Generative AI Services:

12.1 Disclaimer. **Workspace Generative AI Services (a) use emerging technology, (b) may provide inaccurate or offensive Generated Output; and (c) may provide content that does not represent Google's views. Generated Output is not designed for or intended to meet the Customer's regulatory, legal or other obligations, or to be used or relied upon, as a substitute for medical, legal, financial or other professional advice.**

12.2 Similar Generated Outputs. The Customer acknowledges that Workspace Generative AI Services may, in some scenarios, produce the same or similar Generated Output for multiple Customers.

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

12.4 Use Restriction. The Customer will not, and will not allow End Users to, use Generated Output (a) as a material input for the development of models that compete with Workspace Generative AI Services or other Google Workspace Services; or (b) to reverse-engineer or extract components of any Google Workspace Service or their models (except to the extent that such restriction is expressly prohibited by applicable law).

12.5 Usage and availability of the Services. The Customer understands and agrees that (a) it will not, and will not allow End Users to, use Workspace Generative AI Services in a manner that exceeds the limits specified by Google, and (b) use of Workspace Generative AI Services is subject to the availability of the Services, as described at

<https://support.google.com/a/answer/13853332>.

12.6 Age restrictions. The Customer will not allow End Users under the age of 18 to use Workspace Generative AI Services. Notwithstanding the foregoing, if the Customer has Google Workspace for Education Fundamentals, Google Workspace for Education Standard or Google Workspace for Education Plus, then subject to this Section 12.6 (Age restrictions), the Customer may enable End Users under the age of 18 to access and use Gemini for Education and NotebookLM in compliance with the terms of the Agreement, and the Customer must comply with and will remain responsible for its obligations under applicable law related to such access and use, including under Applicable Privacy Law (as defined by the Cloud Data Processing Addendum). Even if the Customer is using one of the foregoing

editions of Google Workspace for Education, End Users under the age of 18 may not access Google AI Pro for Education (and the enhanced artificial intelligence features of Gemini for Education and NotebookLM made available in conjunction with Google AI Pro for Education), as described at <https://support.google.com/gemini/answer/14620100>.

12.7 Healthcare restrictions. The Customer will not, and will not allow End Users to, use Workspace Generative AI Services for clinical purposes (for clarity, non-clinical research, scheduling or other administrative tasks are not restricted), to provide medical advice, medical treatment or diagnosis; or in any manner that is overseen by or requires clearance or approval from any clinical, medical, healthcare or other regulatory authority.

12.8 Suspected violations. Google may immediately suspend or terminate the Customer's use of Workspace Generative AI Services based on any suspected violation of subsections (12.4) to (12.7) above.

12.9 Restrictions. The restrictions contained in subsections (12.6) and (12.7) above are deemed to be 'Restrictions' or 'Use Restrictions' under the applicable Agreement.

12.10 Additional Google indemnification obligations.

(a) Generated Output. Google's indemnification obligations under the Agreement also apply to allegations that an unmodified Generated Output from a Generative AI Indemnified Service infringes a third party's Intellectual Property Rights. This subsection (a) (Generated Output) does not apply if the allegation relates to a Generated Output where:

- (i) the Customer creates or uses such Generated Output that it knew or should have known was likely infringing;
- (ii) the Customer (or Google at the Customer's instruction) disregards, disables or circumvents source citations, filters, instructions or other tools that Google makes available to help the Customer create or use Generated Output responsibly;
- (iii) the Customer uses such Generated Output after receiving notice of an infringement claim from the rights holder or its authorised agent; or
- (iv) the allegation is based on a trademark-related right as a result of the Customer's use of such Generated Output in trade or commerce.

'Generative AI Indemnified Service' means a Service or feature listed at <https://cloud.google.com/terms/generative-ai-indemnified-services>, where the use of such Service or feature is paid for by the Customer and not subject to credits or Free Tier usage.

(b) Training data. Google's indemnification obligations under the Agreement also apply to

allegations that Google's use of training data to create any Google model utilised by a Generative AI Service infringes a third party's Intellectual Property Rights. This indemnity does not cover allegations related to a specific Generated Output, which may be covered by subsection (a) (Generated Output) above.

12.11 Training restriction. Google will not use Customer Data to train or fine-tune any of its generative artificial intelligence models supporting the Google Workspace Generative AI Services without the Customer's prior permission or instruction.

12.12 Additional definitions.

'Generated Output' means the data or content generated or received by the Customer or its End Users via Workspace Generative AI Services under the Customer's Workspace account, as prompted by data or content submitted by them via those services. Generated Output is Customer Data. As between the Customer and Google, Google does not assert any ownership rights in any new intellectual property created in the Generated Output.

'Workspace Generative AI Services' includes (i) Gemini in Workspace (formerly known as Gemini for Google Workspace) and (ii) other generative artificial intelligence features or functionality of the Google Workspace Services.

13. **User Experience Research.** If the Customer enrolls in the Google Cloud User Experience Research Programme for Google Workspace, the Customer's participation will be subject to the Google Cloud User Experience Research Panel Addendum available at <https://cloud.google.com/terms/user-experience-research>.

14. **Client-side encryption.** As between Google and the Customer, the Customer bears sole responsibility for all aspects of the external encryption key management service chosen by the Customer, including all encryption keys generated by it for use with client-side encryption. Notwithstanding any term to the contrary in the CDPA, Google will be unable to recover any encryption key or any Customer Data encrypted by that encryption key if the encryption key is lost, stolen or corrupted. Client-side encryption will become entirely unavailable for all applicable Services if the external key management service is interrupted or becomes inaccessible.

15. **eSignature.** The following terms apply only to the electronic signature feature in Google Docs and Google Drive ('eSignature'):

15.1 In-Scope Editions. eSignature is included in the following Google Workspace editions:

- (a) all Google Workspace Business editions (excluding Google Workspace Business Starter);
- (b) all Google Workspace Enterprise editions;

- (c) all Google Workspace Essentials editions (excluding Google Workspace Essentials Starter); and
- (d) Google Workspace for Education Plus.

15.2 Transacting electronically. By using eSignature, the Customer or End Users will transact electronically with counterparties to the relevant document (who may themselves be End Users). For clarity, Google's provision of eSignature does not make Google a party to, or bind Google under, any document signed or executed via eSignature (an 'eSigned Document').

15.3 Responsibility for contents and legal requirements. When using eSignature for document signature or execution, the Customer and End Users are responsible for:

- (a) the contents of the document;
- (b) verifying that applicable law in all relevant jurisdictions permits electronic (rather than 'wet ink') signature or execution of the document; and
- (c) ensuring compliance with any signature or execution formalities required for legal validity or enforceability of the document in all relevant jurisdictions, including formalities related to the nature of the document (e.g. requirements for witnesses).

15.4 Disclaimer. Google expressly disclaims, to the fullest extent permitted by applicable law, any warranties of any kind or any representations related to the legal validity or enforceability of any eSigned Document in any jurisdiction.

15.5 Signer's identity and authority. The Customer and End Users are responsible for verifying the identity, email address and signature authority of any recipient of an eSignature request. The Customer is responsible for ensuring that only duly authorised End Users use eSignature to sign or execute documents on behalf of the Customer.

15.6 Signer terms. The recipient of an eSignature request may need to accept separate terms (including the Google Terms of Service (<https://policies.google.com/terms?hl=en-GB>) and eSignature Additional Terms of Service for Signers (https://workspace.google.com/intl/en_uk/terms/google-workspace-individual-terms/esignature-signer/) or eSignature Additional Terms of Service

(https://workspace.google.com/intl/en_uk/terms/google-workspace-individual-terms/esignature/)), but any eSignature request received by an End User will be governed by the Agreement.

15.7 Copies and storage of eSigned Documents.

- (a) Google will attempt to email copies of eSigned Documents to all signatories and to add copies to their Google Drive accounts but cannot guarantee receipt (e.g. spam filters may block Google's email,

or signatories may not have Drive accounts or sufficient storage).

(b) The Customer and End Users are responsible for retaining copies of eSigned Documents; backing up those copies as appropriate; and verifying, after they send eSignature requests or change access permissions to Google Drive copies of eSigned Documents, that all counterparties have received and retain copies of eSigned Documents.

15.8 Signature information and document access. Copies of eSigned Documents (including their audit trails) may contain: certificate-based signatures that help identify the parties; email addresses of signatories; information about signatories' Google Accounts (e.g. pseudonymised identifiers) and devices (e.g. IP addresses) and other details (e.g. times and dates of signatures). Without prejudice to Google's obligations under the Cloud Data Processing Addendum, the Customer and End Users acknowledge that anyone with access to the eSigned Document will have access to the information described in this section.

15.9 Regional Terms for eSignature.

Brazil. The use of eSigned Documents may involve heightened enforceability risks in Brazil. As described in Section 15.3 (Responsibility for contents and legal requirements), and without limiting any obligations under that section, the Customer and End Users are responsible for verifying whether Brazilian law permits the use of eSignature as a valid means of signing or executing contracts.

16. Assured Controls.

16.1 General. Google will provide TSS for Assured Controls and Assured Controls Plus in accordance with Customer-selected controls and features of the Services as described at <https://support.google.com/a/answer/13880647?hl=en>. It is the Customer's responsibility to determine whether Customer-selected controls and features are adequate for the Customer's purposes.

16.2 Google personnel access controls. Assured Controls and Assured Controls Plus features (such as Access Approval and Access Management features) enable the Customer to prevent Google personnel located outside the Customer-selected Data Region (described in Section 1 (Data Regions) above) from accessing certain primary data stored at-rest within Customer Data that is stored in an Assured Controls or Assured Controls Plus environment ('Covered Data'), as described at <https://support.google.com/a/answer/10379605?sjid=5723963757357736231-NA>.

17. Storage limits. The Customer understands and agrees that it will not, and will not allow End Users to, use any Google Workspace Services (including,

without limitation, the Workspace Generative AI Services) in a manner that exceeds the storage limits specified for the Customer's edition of Google Workspace, as described at

https://support.google.com/a?p=storage_by_edition. Google may suspend the Customer's account based on any violation of this section.

18. reCAPTCHA notice requirement. The Customer agrees to explicitly inform Customer End Users that use of reCAPTCHA in connection with Google Meet is subject to the Google Privacy Policy

(<https://policies.google.com/privacy>) and Terms of Service

(<https://policies.google.com/terms>). Google collects hardware and software information, such as device and application data, through reCAPTCHA only as necessary to provide, maintain and improve reCAPTCHA, and for general security purposes. Such information will not be used for any other purpose, such as personalised advertising by Google.

19. Price change rationale. To the extent that Google has a right to modify Prices under the Agreement, it may have various reasons for doing so, including (for example, and without limitation): (a) changes in Google's underlying costs for developing, providing, maintaining and/or selling the Services, such as costs related to hardware, software licences, energy, labour and data centre infrastructure; (b) enhancements, modifications or changes to the nature, features or functionality of the Services, including the introduction of new services or capabilities; (c) prevailing market conditions, including competitive pressures, inflation, deflation or currency exchange rate fluctuations; (d) changes in applicable laws, regulations, taxes or other compliance requirements that impact the cost or manner of delivering the Services; (e) the evolution of technology and industry standards affecting the Services; and (f) changes to costs payable by Google to third parties.

20. Google Workspace for Education. The following terms apply only to the Google Workspace for Education editions:

20.1 Customer responsibility. The Customer is solely responsible for monitoring and auditing its End User Accounts and promptly (a) removing or reassigning End User Accounts when no longer in use (including all Inactive Accounts (defined below)); and (b) deleting or exporting Customer Data (including Customer Data associated with Inactive End User Accounts) and removing End User Accounts (including Inactive Accounts) as required to comply with applicable law.

20.2 Customer instruction. In support of its obligations above, the Customer instructs Google to, in line with Google's procedures, suspend or delete the Customer Data associated with any Inactive End User Account (defined below) or Inactive Domain (defined below).

20.3 Additional definitions.

'Inactive Account' means an Inactive Domain or Inactive End User Account.

'Inactive Domain' means a Domain Email Address or Domain Name that for an uninterrupted period of at least two years has had no active End User

Accounts (i.e. it has had no Accounts other than Inactive End User Accounts).

'Inactive End User Account' means an End User Account that has not been used or logged in to by the Customer or the relevant End User for an uninterrupted period of at least two years. Use by the Customer or End User may include activities such as (i) reading or sending an email, (ii) using Google Drive, (iii) watching a YouTube video, (iv) sharing a photo, (v) downloading an app, (vi) using Google Search, or (vii) using Sign in with Google to sign in to a third-party app or service.

21. Resold Customers. This Section 21 (Resold Customers) applies only if (a) the Customer orders the Services from a Reseller under a Reseller Agreement (such Services, 'Resold Services') and (b) the Customer has a direct agreement with Google to provision those Resold Services.

21.1 Additional definitions

'Reseller' means, if applicable, the authorised unaffiliated third-party reseller that sells the Services to the Customer.

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

'Reseller Fees' means the fees (if any) for Services used or ordered by the 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 the Customer and the Reseller specifying the Services that the Customer is ordering from the Reseller.

21.2 Applicable terms. For the purposes of Resold Services:

(i) The Section of the Agreement entitled 'Payment Terms' will not apply, nor will any provisions in the applicable Service-Specific Terms relating to billing, invoicing or payment;

(ii) Reseller Fees will apply and be payable directly to the Reseller, and all prices for Resold Services will be solely determined between the Reseller and Customer;

(iii) Google will provide to the Customer the Resold Services described in the Reseller Order to the extent that there is a valid and binding order for such Services between Google and the Reseller;

(iv) The Customer will receive any applicable SLA credits or monetary refunds described in this Agreement from the Reseller only (and the Customer

must notify the Reseller if Google fails to meet any SLA);

(v) Notwithstanding Google's support obligations in the TSS Guidelines, Google will not provide any support to the Customer unless (A) the Customer orders TSS from Google directly or (B) the Reseller orders TSS from Google on behalf of the Customer, and such TSS entitlement requires Google to provide TSS directly to the Customer. All other support (if any) will be provided to the Customer by the Reseller in accordance with the Reseller Agreement, subject to Section 14(e) (Reseller technical support);

(vi) the Customer acknowledges that access to the Services may be suspended if at any time the Reseller or Customer fails to maintain a billing account linked to the Customer's Account;

(vii) In the event of termination of this Agreement, Google will send the Reseller (and not the Customer) the final invoice (if applicable) for payment obligations related to Resold Services. Customer will notify (A) the Reseller of any termination of this Agreement and (B) Google of any termination of the Reseller Agreement;

(viii) Any renewal(s) of the Resold Services and/or any Reseller Order will be as agreed between the Customer and Reseller;

(ix) If the Reseller fails to pay an undisputed invoice for Resold Services to Google due to the Customer's failure to pay the Reseller, Google may suspend the Customer's access to the Services;

(x) To the extent that any Customer Data is under the Reseller's organisational resource, then notwithstanding anything to the contrary in this Agreement (including the Cloud Data Processing Addendum):

(A) the Cloud Data Processing Addendum will not apply with respect to the processing and security of such Customer Data;

(B) Google will only access, use and otherwise process such Customer Data in accordance with the separate agreement between Google and the Reseller (including its then-current terms describing data processing and security of 'Partner Data' as defined by that agreement) and will not access,

use or process such Customer Data for any other purpose; and

(C) the consents and notices for which the Customer is responsible under the section of this Agreement titled 'Privacy' or 'Consents' must also permit accessing, storing and processing of Customer Data as described in subsection (B) above.

(xi) The Google Cloud Platform Services require linking to the Reseller's billing account in order to be billed by the Reseller. The Customer acknowledges and agrees that, (A) if the Google's agreement with the Reseller or Customer's Reseller Agreement is terminated or expires, then the Services will no longer be linked to the Reseller's billing account, and (B) unless any such Services used by Customer are linked to the Reseller's billing account, such Services will (x) not constitute Resold Services (and therefore not be subject to this Section 14 (Resold Customers)), and (y) be regarded as Services ordered directly from Google and accordingly, despite the terms of the Reseller Agreement (including the fees agreed between the Customer and Reseller), the Customer will be required to pay Fees to Google for such Services, in accordance with the terms of this Agreement.

(xii) 'Cloud Data Processing Addendum', as it is used in this Agreement, means the then-current terms describing data processing and security obligations with respect to Customer Data that is under the Customer's (not Reseller's) organisational resource, as described at <https://cloud.google.com/terms/data-processing-addendum>.

(xiii) 'Order Term', as it is used in this Agreement, means the period of time starting on the Services Start Date or the renewal date (as applicable) for the Resold Services and continuing until the expiry or termination of the applicable Reseller Order; and (xiv) 'Services Start Date', as it is used in this Agreement, means either the start date described in the Reseller Order or, if none is specified in the Reseller Order, the date that Google makes the Resold Services available to the Customer.

21.3 Liability cap. For the purposes of the section of the Agreement titled 'Limitation on amount of Liability', where the event giving rise to Liability is a breach of this Agreement or otherwise arises in connection with the Resold Services, 'Fees'

as it is used in that Section means 'Reseller Fees'. If the Customer or Google brings a claim under the Agreement, then, for the purposes of establishing the Liability cap under the section of the Agreement titled 'Limitation on amount of Liability', upon Google's request, the Customer will (i) promptly disclose to Google the amount of any Reseller Fees paid or payable under the Reseller Agreement; (ii) consent to the Reseller disclosing such amount to Google, notwithstanding the Reseller's confidentiality obligations under the Reseller Agreement; and (iii) procure any consents necessary to enable the Customer's or Reseller's disclosure under this Section 14(c) (Liability cap). Subject to the section of the Agreement titled 'Unlimited Liabilities', Google will not be liable for damages under this Agreement to the extent that the Customer has claimed damages from the Reseller in respect of the same event or series of events.

21.4 Sharing Confidential Information. Google may share Customer Confidential Information with the Reseller as a Delegate subject to the section of the Agreement titled 'Confidentiality' or 'Confidential Information'.

21.5 Reseller-Customer relationship. At the Customer's discretion, the Reseller may access the Customer's Account. As between Google and the Customer, the Customer is solely responsible for (i) any access by the Reseller to the Customer's Account; (ii) defining in the Reseller Agreement any rights or obligations as between the Reseller and Customer with respect to the Resold Services; and (iii) verifying whether data provided to Google by the Customer or End Users through the Resold Services under the Account, and data that the Customer or End Users derive from that data through their use of the Resold Services, will be under Customer's or Reseller's organisational resource. Google will not have any Liability arising out of a Reseller's (A) suspension or termination of the Customer's access to the Services; (B) access to and visibility of the Customer's Account and the Customer's Account's billing-related metadata; or (C) offering or provisioning of the Reseller or third-party products or services.

21.6 Reseller technical support. Customer acknowledges and agrees that the Reseller may disclose Customer and End User personal data to Google as reasonably required for the Reseller to handle any support issues that the Customer escalates to or via the Reseller.

22. Regional Terms.

22.1 Japan. If the Customer's billing address is in Japan, then Gmail, Chat and Meet will be provided by Google Connect Asia Pacific Pte. Ltd. ('GCAP'), although invoices will still be sent by Google Asia Pacific Pte. Ltd. In relation only to the foregoing Services, Google Asia Pacific Pte. Ltd. is a duly authorised agent of GCAP and contracts on behalf of GCAP.



22.2 France. The Customer will comply with France's General Security Policy for Health Information Systems (PGSSI-S) to the extent applicable.

Previous Versions

Last modified 13 October 2025

28 October 2025

16 October 2025

13 October 2025

7 October 2025

9 September 2025

28 August 2025

30 June 2025

17 June 2025

2 April 2025

17 March 2025

18 February 2025

3 January 2025

15 October 2024

3 June 2024

21 February 2024

20 November 2023

12 October 2023

14 August 2023

31 May 2023

3 May 2023

11 January 2023

31 October 2022

11 October 2022

22 September 2022

19 September 2022

7 July 2022

31 March 2022

15 March 2022

1 February 2022

30 September 2021

3 June 2021

14 April 2021

21 December 2020

6 October 2020



Service Specific Terms for Looker (original)

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

These Service Specific Terms applicable to Looker (original) Services are incorporated into the agreement under which Google has agreed to provide Looker (original) to Customer (the "Agreement"). If the Agreement authorizes you to resell or supply Looker (original) under a Google Cloud partner or reseller program, then except for in the section entitled "Partner-Specific Terms", all references to Customer in the Service Specific Terms refer to you ("Partner" or "Reseller", as used in the Agreement), and all references to Customer Data in the Service Specific Terms mean Partner Data. If you are accessing the Services as a customer of an unaffiliated Google Cloud reseller, then Section 9 (Resold Customers) applies to you. Capitalized terms used but not defined in these Service Specific Terms for Looker (original) have the meaning stated in the Agreement.

1. Customer's Use of the Services

A. Access to the Services. Google will provide the Services to Customer by (a) providing access to an Instance for a Looker Hosted Deployment or (b) providing a license key for a Customer Hosted Deployment. Customer may configure the Services for Internal Business Purposes and External Business Purposes only to the extent authorized in the Order Form.

B. External Business Users. 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.



C. *Services and Software Use Review.* Within 30 days of Google's reasonable written request, Customer will provide a sufficiently detailed written usage report describing its usage of the Services and Software in accordance with the applicable Scope of Use, with any details reasonably requested by Google. If requested, Customer will provide reasonable assistance and access to information to verify the accuracy of any information provided to Google. If the review indicates that Customer has exceeded the number of End Users, Scope of Use, or Deployment Attributes set forth in the applicable Order Form, or if Google otherwise determines such excessive usage, then the parties agree to discuss in good faith the additional Fees due by Customer to Google for such over-deployment. The agreed-upon additional Fees associated with the over-deployment will be memorialized in a new Order Form or otherwise invoiced by Google.

D. *Additional Deployment Attributes.* Customer may purchase additional Deployment Attributes (including adding End Users) during an Order Term by executing a new 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 an Order Term. This section will not apply if Customer has purchased the Services from an Unaffiliated Cloud Marketplace pursuant to Section 4 (Unaffiliated Cloud Marketplace) of these Service Specific Terms.

E. *Hosting Locations.* Notwithstanding any commitments made by Google in the Agreement (including in any Order Form) with respect to hosting the Services or storing Customer Data in a specific location or region, certain features of the Services may not support such hosting and data storage commitments. Any such excluded feature will be listed in the Documentation.

2. Software Terms

A. *Software License.* Google grants Customer a non-exclusive, non-sublicensable, non-transferable license during the Term to reproduce and use the Software ordered by Customer on systems owned, operated, or managed by or on behalf of Customer in accordance with (i) the Agreement, and (ii) if applicable, the Scope of Use.

B. *Open Source or Third Party Terms.* If the Software contains open source or third-party components, those components may be subject to separate license agreements, which Google will make available to Customer. Customer is solely responsible for complying with the terms of any such third party components or open source licenses.

C. *Termination.* On termination or expiration of the Agreement, Customer will stop using all Software and delete all copies.

D. *Other Warranties and Compliance.* Each party represents and warrants that it will comply with all laws applicable to its provision or use of the Software. Customer will: (i) ensure that Customer and its End Users' use of the Software complies with the Agreement (including the Scope of Use) and the restrictions in the Agreement applying to Customer's use of the Services; (ii) use commercially reasonable efforts to prevent and terminate any unauthorized access to or use of the Software; and (iii) promptly notify Google of any unauthorized access to or use of the Software of which Customer becomes aware.

E. *Software Indemnification.* Google's Intellectual Property Rights infringement indemnity obligations under the Agreement apply to Software, and Customer's indemnity obligations under the Agreement with respect to Customer's use of the Services apply to Customer's use of Software. In addition to any other indemnity



exclusions in the Agreement, Google's indemnity obligations will not apply to the extent the underlying allegation arises from modifications to Software not made by Google or use of versions of Software that are no longer supported by Google.

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

G. *Scope of Use Compliance*. Software may transmit to Google metering information reasonably necessary to verify that use of the Software complies with the Scope of Use. Customer will not disable or interfere with the transmission of such metering information.

3. Pre-GA Offerings Terms

Google may make available to Customer pre-general availability Looker (original) features, services, or software that are identified as "Early Access", "Alpha", "Beta", "Preview", "Experimental", or a similar designation through the Services, in the Documentation or related materials, or a Test Application (as defined below)(collectively, "Pre-GA Offerings"). While Pre-GA Offerings are not Services, Customer's use of Pre-GA Offerings is subject to the terms of the Agreement applicable to Services, as amended by this Section 3.

A. *Access to and use of Pre-GA Offerings*.

1. *Enabling Pre-GA Offerings*. If Google accepts Customer as a test user of any Pre-GA Offerings (based on Google's then-current domain level requirements for test users), Google will make those Pre-GA Offerings available for use by Customer subject to the terms of this Section 3 (Pre-GA Offerings Terms). Customer may opt into being a test user of one or more Pre-GA Offerings via permissions granted by Customer via the Services. Notwithstanding the preceding sentence, certain Pre-GA Offerings may be enabled in the Services by default. These Pre-GA Offerings will be available to Customer unless Customer disables the Pre-GA Offerings via the Services. Google will notify Customer prior to enabling any Pre-GA Offerings by default. Additional terms ("Specific Test Terms") may apply to any Pre-GA Offering. If so, these Specific Test Terms will be provided by Google in writing before any use of the Pre-GA Offering by Customer. The Specific Test Terms are incorporated into this Section 3.

2. *Use of Customer Test Data*. Google may, and Customer will (including by collecting or providing any required consents or notices) ensure that Google may use any Customer Data (including Customer Personal *Data*) submitted, stored, sent or received via any Pre-GA Offerings by Customer or its End Users ("Customer Test Data") to provide, test, analyze, develop and improve those Pre-GA Offerings and any Google products and services used with them without any restriction or obligation to Customer, any End User or any third party, other than as stated in the Agreement's confidentiality provisions and below.

3. *Application of the Cloud Data Processing Addendum.* If Customer has accepted, or the parties have otherwise agreed, to Google's then-current terms describing data protection and processing obligations with respect to Customer Data at <https://cloud.google.com/terms/data-processing-addendum> (the "Cloud Data Processing Addendum" or "CDPA"), it will apply to Pre-GA Offerings as "Services" for purposes of the CDPA. Unless stated otherwise in the applicable Pre-GA Offerings, the entirety of this Section 3 (Pre-GA Offerings Terms) will form part of the "Agreement" referred to in Section 5.2 (Compliance with Customer's Instructions) of the CDPA, subject to the following amendments:

- i. Customer acknowledges that, for purposes of Section 6.1 (Deletion by Customer) of the CDPA and to the extent permitted by applicable law, the functionality of the Pre-GA Offerings may not allow deletion of Customer Test Data during the period during which Customer is permitted to use the Pre-GA Offerings ("Pre-GA Term"), but that Customer Test Data will be deleted upon expiration of the Pre-GA Term in accordance with Section 6.2 (Return or Deletion When Term Ends) of the CDPA;
- ii. Unless stated otherwise in the Test Application or Specific Test Terms, information about Subprocessors (as defined in the CDPA) engaged in relation to Pre-GA Offerings will be made available in writing by Google upon Customer's request;
- iii. Google will inform Customer of the engagement during the Pre-GA Term of any new third-party Subprocessor in relation to the Pre-GA Offerings by sending an email to the Notification Email Address before the new Subprocessor starts processing any Customer Test Data. Customer may, as its sole and exclusive remedy if Customer objects to the Subprocessor, cease using the applicable Pre-GA Offerings; and
- iv. Pre-GA Offerings are not "Audited Services" under the CDPA.

4. *Use Restrictions.* Customer will not, and will not allow End Users to: (i) use Pre-GA Offerings to process Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996, or (ii) use Pre-GA Offerings to process data subject to legal or regulatory compliance requirements.

B. *Change, Suspension, or Discontinuance.* Pre-GA Offerings (including any of their features) may be changed, suspended or discontinued at any time without prior notice to Customer.

C. *Disclaimer.* PRE-GA OFFERINGS ARE PROVIDED 'AS IS', WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS OF ANY KIND, AND ARE NOT COVERED BY ANY SLA OR GOOGLE INDEMNITY. Except as otherwise indicated in Specific Test Terms for a given Pre-GA Offering, Pre-GA Offerings are not covered by TSS.

D. *Liability.* Google will not be liable for any amounts in excess of the lesser of (A) the limitation on the amount of liability stated in the Agreement or (B) \$25,000. Nothing in the preceding sentence will affect exclusions from any limitation of liability in the Agreement with respect to the following: (1) death or personal injury resulting from negligence, (2) fraud or fraudulent misrepresentation, (3) infringement of the other party's Intellectual Property Rights, or (4) matters for which liability cannot be excluded or limited under applicable law.



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

F. *Termination*. Either party may terminate Customer's use of a Pre-GA Offering at any time with written notice to the other party.

4. Unaffiliated Cloud Marketplace

This Section 4 (Unaffiliated Cloud Marketplace) applies only if Customer orders Looker Services from an Unaffiliated Cloud Marketplace (such Looker Services, "UCM Services"). For the purposes of UCM Services:

A. The section of the Agreement entitled "Payment Terms" will not apply.

B. Fees for UCM Services will apply and be payable directly to the provider of the Unaffiliated Cloud Marketplace.

C. Google and Customer will agree upon pricing and quantities for the UCM Services in advance of Customer placing an order for the UCM Services with the provider of the Unaffiliated Cloud Marketplace (such order, a "UCM Order"), and Google will provide to Customer the agreed-upon UCM Services after Customer places the UCM Order.

D. Customer will receive any applicable SLA credits or monetary refunds described in this Agreement from the provider of the Unaffiliated Cloud Marketplace only.

E. Any renewal(s) of the UCM Services will be as agreed between Customer and Google.

F. For the purpose of this Section 4 (Unaffiliated Cloud Marketplace), the following definitions apply:

"Order Term", as it is used in this Agreement with respect to UCM Services, means the period of time starting on the Services Start Date or the renewal date (as applicable) for the UCM Services and continuing until the expiration or termination of the applicable UCM Order.

"Services Start Date", as it is used in this Agreement with respect to UCM Services, means either the start date described in the UCM Order or, if none is specified in the UCM Order, the date Google makes the UCM Services available to Customer.

"Unaffiliated Cloud Marketplace" means an online cloud marketplace that is not owned or managed by Google or its Affiliates.

5. Third-Party Offerings

The Looker Marketplace includes software and services that are not owned by Google. Customer's use of such software or services is governed by a separate agreement between Customer and the third party provider. Customer may need to accept third party terms and conditions before accessing or downloading such software or services via the Looker Marketplace. Customer acknowledges and agrees that Google is not responsible for, and makes no representations or warranties regarding the installation, integration, interoperability, functionality or content of any third party software or services provided via the Looker Marketplace.

6. Third-Party Terms

The Oracle JDBC software components used in conjunction with the Services are subject to the terms and conditions stated at <https://cloud.google.com/terms/looker/legal/customers/service-terms/oracle>.

7. Google Maps Visualizations

Looker (original) visualizations include Google Maps features and content that are subject to the then-current versions of the: (1) Google Maps/Google Earth Additional Terms of Service at https://maps.google.com/help/terms_maps.html; and (2) Google Privacy Policy at <https://www.google.com/policies/privacy/> (together, the "Google Maps Terms"). To the extent Customer includes Google Maps features and content in the Looker (original) Services under an External Business Purposes deployment, Customer will include the Google Maps Terms in the contract governing use of that Customer Application by PBL Client and its users. For the avoidance of doubt, the Looker (original) visualizations features that use Google Maps do not share any Customer Data with Google Maps.

8. Looker Generative AI Services

A. *Disclaimers.*

Looker Generative AI Services (i) use emerging technology, (ii) may provide inaccurate or offensive Generated Output; and (iii) may provide content that does not represent Google's views. Generated Output is not designed for or intended to meet Customer's regulatory, legal, or other obligations, or to be used, or relied upon, as a substitute for medical, legal, financial, or other professional advice.

Looker Generative AI Services are part of Gemini for Google Cloud and may not support the same compliance and security offerings as Looker (original) Services or your other data sources, including data residency controls. Only enable Looker Generative AI Services for Instances or Projects (with respect to Looker Studio Pro) that require compliance offerings where the requisite compliance offerings are supported by Gemini for Google Cloud. See here (<https://docs.cloud.google.com/gemini/docs>) for more information.

B. *Similar Generated Outputs.* Customer acknowledges that Looker Generative AI Services may, in some scenarios, produce the same or similar Generated Output for multiple Customers.

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

D. *Use Restriction.* Customer will not, and will not allow End Users to, use Generated Output (i) as a material input for the development of models that compete with Looker Generative AI Services or other Looker (original) Services; or (ii) to reverse engineer or extract components of any Looker (original) Services or their models (except to the extent such restriction is expressly prohibited by applicable law).

E. *Usage and Availability of the Services.*

Customer understands and agrees that it will not, and will not allow End Users to, use Looker Generative AI Services in a manner that exceeds the limits specified by Google.

Gemini in Looker is only available for Looker Hosted Deployments.

F. *Age Restrictions.* Customer will not allow End Users under the age of 18 to use Looker Generative AI Services.

G. *Healthcare Restrictions.* Customer will not, and will not allow End Users to, use Looker Generative AI Services for clinical purposes (for clarity, non-clinical research,

scheduling, or other administrative tasks are not restricted), to provide medical advice, medical treatment, or diagnosis; or in any manner that is overseen by or requires clearance or approval from any clinical, medical or healthcare or other regulatory authority.

H. *Suspected Violations*. Google may immediately suspend or terminate Customer's use of Looker Generative AI Services based on any suspected violation of subsections (8.D) through (8.G) above.

I. *Restrictions*. The restrictions contained in subsections (8.F) and (8.G) above are deemed to be "Restrictions" or "Use Restrictions" under the applicable Agreement.

J. *Additional Google Indemnification Obligations*.

Generated Output. Google's indemnification obligations under the Agreement also apply to allegations that an unmodified Generated Output from a Generative AI Indemnified Service infringes a third party's Intellectual Property Rights. This subsection (1) (Generated Output) does not apply if the allegation relates to a Generated Output where: (i) Customer creates or uses such Generated Output that it knew or should have known was likely infringing, (ii) Customer (or Google at Customer's instruction) disregards, disables, or circumvents source citations, filters, instructions, or other tools Google makes available to help Customer create or use Generated Output responsibly, (iii) Customer uses such Generated Output after receiving notice of an infringement claim from the rightsholder or its authorized agent, or (iv) the allegation is based on a trademark-related right as a result of Customer's use of such Generated Output in trade or commerce. "Generative AI Indemnified Service" means a Service or feature listed at <https://cloud.google.com/terms/generative-ai-indemnified-services>, where the use of such Service or feature is paid for by Customer and not subject to credits or free tier usage.

Training Data. Google's indemnification obligations under the Agreement also apply to allegations that Google's use of training data to create any Google model utilized by a Generative AI Service infringes a third party's Intellectual Property Rights. This indemnity does not cover allegations related to a specific Generated Output, which may be covered by subsection (1) (Generated Output) above.

K. *Training Restriction*. Google will not use Customer Data to train or fine-tune any of its generative artificial intelligence models supporting the Looker Generative AI Services without Customer's prior permission or instruction.

L. *Modifying, Disregarding, or Disabling Safety Filters*. Google makes available safety filters for certain Looker Generative AI Services. Customer is solely responsible for (i) its use, non-use, or modification (including modifications made by Google at Customer's instruction) of safety filters in creating Generated Output, and (ii) disregarding safety instructions or Documentation.

M. *Definitions*.

"*Generated Output*" means the data or content generated or received by Customer or its End Users via Looker Generative AI Services under the Customer's Account, as prompted by data or content submitted by them via those services. Generated Output is Customer Data. As between Customer and Google, Google does not assert any ownership rights in any new intellectual property created in the Generated Output.



"*Looker Generative AI Services*" includes (i) Gemini in Looker and (ii) other generative artificial intelligence features or functionality of Looker (original). "Project" has the meaning given in the Agreement with respect to GCP Services.

9. Resold Customers

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

a. Applicable Terms. For the purposes of Resold Services:

(i) The Section of the Agreement entitled "Payment Terms" will not apply, nor will any provisions in the applicable Service Specific Terms relating to billing, invoicing, or payment;

(ii) Reseller Fees will apply and be payable directly to Reseller, and all prices for Resold Services will be solely determined between Reseller and Customer;

(iii) Google will provide to Customer the Resold Services described in the Reseller Order to the extent that there is a valid and binding order for such Services between Google and Reseller;

(iv) Customer will receive any applicable SLA credits or monetary refunds described in this Agreement from Reseller only (and Customer must notify Reseller if Google fails to meet any SLA);

(v) Notwithstanding Google's support obligations in the TSS Guidelines, Google will not provide any support to Customer unless (A) Customer orders TSS from Google directly or (B) Reseller orders TSS from Google on behalf of Customer, and such TSS entitlement requires Google to provide TSS directly to Customer. All other support (if any) will be provided to Customer by Reseller in accordance with the Reseller Agreement, subject to Section 9(e) (Reseller Technical Support);

(vi) Customer acknowledges that access to the Services may be Suspended if at any time Reseller or Customer fails to maintain a billing account linked to Customer's Account;

(vii) In the event of termination of this Agreement, Google will send Reseller (and not Customer) the final invoice (if applicable) for payment obligations related to Resold Services. Customer will notify (A) Reseller of any termination of this Agreement and (B) Google of any termination of the Reseller Agreement;

(viii) Any renewal(s) of the Resold Services and/or any Reseller Order will be as agreed between Customer and Reseller;

(ix) If Reseller fails to pay an undisputed invoice for Resold Services to Google due to Customer's failure to pay Reseller, Google may Suspend Customer's access to the Services;

(x) To the extent that any Customer Data is under Reseller's organizational resource, then notwithstanding anything to the contrary in this Agreement (including the Cloud Data Processing Addendum):

(A) the Cloud Data Processing Addendum will not apply with respect to the processing and security of such Customer Data;

(B) Google will only access, use, and otherwise process such Customer Data in accordance with the separate agreement between Google and Reseller (including its then-current terms describing data processing and security of

"Partner Data" as defined by that agreement) and will not access, use, or process such Customer Data for any other purpose; and
(C) the consents and notices for which Customer is responsible under the section of this Agreement titled "Privacy" or "Consents" must also permit accessing, storing, and processing of Customer Data as described in subsection (B) above.

(xi) The Looker (original) Services require linking to the Reseller's billing account in order to be billed by the Reseller. Customer acknowledges and agrees that, (A) if Google's agreement with the Reseller or Customer's Reseller Agreement is terminated or expires, then the Services will no longer be linked to the Reseller's billing account, and (B) unless any such Services used by Customer are linked to the Reseller's billing account, such Services will (x) not constitute Resold Services (and therefore not be subject to this Section 9 (Resold Customers)), and (y) be regarded as Services ordered directly from Google and accordingly, despite the terms of the Reseller Agreement (including the fees agreed between Customer and Reseller), Customer will be required to pay Fees to Google for such Services, in accordance with the terms of this Agreement.

(xii) "Cloud Data Processing Addendum", as it is used in this Agreement with respect to Resold Services, means the then-current terms describing data processing and security obligations with respect to Customer Data that is under Customer's (not Reseller's) organizational resource, as described at <https://cloud.google.com/terms/data-processing-addendum>.

(xiii) "Order Term", as it is used in this Agreement with respect to Resold Services, means the period of time starting on the Services Start Date or the renewal date (as applicable) for the Resold Services and continuing until the expiration or termination of the applicable Reseller Order; and

(xiv) "Services Start Date", as it is used in this Agreement with respect to Resold Services, means either the start date described in the Reseller Order or, if none is specified in the Reseller Order, the date Google makes the Resold Services available to Customer; and

b. Liability Cap. For the purposes of the section of the Agreement titled "Limitation on Amount of Liability", where the event giving rise to Liability is a breach of this Agreement or otherwise arises in connection with the Resold Services, "Fees" as it is used in that Section means "Reseller Fees". If Customer or Google brings a claim under the Agreement, then, for the purposes of establishing the Liability cap under the section of the Agreement titled "Limitation on Amount of Liability", upon Google's request, Customer will (a) promptly disclose to Google the amount of any Reseller Fees paid or payable under the Reseller Agreement; (b) consent to Reseller disclosing such amount to Google, notwithstanding Reseller's confidentiality obligations under the Reseller Agreement; and (c) procure any consents necessary to enable Customer's or Reseller's disclosure under this Section 9(b) (Liability Cap). Subject to the section of the Agreement titled "Unlimited Liabilities", Google will not be liable for damages under this Agreement to the extent Customer has claimed damages from Reseller in respect of the same event or series of events.

c. Sharing Confidential Information. Google may share Customer Confidential Information with Reseller as a Delegate subject to the section of the Agreement titled "Confidentiality" or "Confidential Information".

d. Reseller-Customer Relationship. At Customer's discretion, Reseller may access Customer's Account. As between Google and Customer, Customer is solely



responsible for (i) any access by Reseller to Customer's Account; (ii) defining in the Reseller Agreement any rights or obligations as between Reseller and Customer with respect to the Resold Services; and (iii) verifying whether data provided to Google by Customer or End Users through the Resold Services under the Account, and data that Customer or End Users derive from that data through their use of the Resold Services, will be under Customer's or Reseller's organizational resource. Google will not have any Liability arising out of a Reseller's (A) suspension or termination of Customer's access to the Services; (B) access to and visibility of Customer's Account and Customer's Account's billing-related metadata; or (C) offering or provisioning of Reseller or third party products or services.

e. Reseller Technical Support. Customer acknowledges and agrees that Reseller may disclose Customer and End User personal data to Google as reasonably required for Reseller to handle any support issues that Customer escalates to or via Reseller.

f. Survival. The following subsections of this Section 9 (Resold Customers) will survive expiration or termination of the Agreement: subsection (a)(vii), subsection (b) (Liability Cap), subsection (c) (Sharing Confidential Information), and subsection (d) (Reseller-Customer Relationship).

10. Currency Conversion

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

11. Additional Definitions

"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.

"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.

"External Business Purposes" or *"PBL"* means the use of the Services or Software embedded in a Customer Application.

"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 third-party hosting facility designated by Google, unless otherwise agreed by the parties in an Order Form. A Looker Hosted Deployment includes the In-Product Services.



"*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.

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

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

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

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

"*Scope of Use*" means any limits on installation or usage of Software or Services described in the Documentation, Order Form, or otherwise presented by Google.

Previous versions (*Last modified November 6, 2025*)

October 13 2025, July 1 2025, April 22 2025, May 8 2023, April 4 2023,
January 4 2023, February 14 2022



Google Cloud Service Level Agreements

Google Cloud Platform

The following are the Service Level Agreements for Google Cloud Platform services.

AI Platform Training and Prediction (https://cloud.google.com/ai-platform/training-and-prediction/sla?hl=en)	AlloyDB (https://cloud.google.com/alloydb/sla?hl=en)
Anti Money Laundering AI (https://cloud.google.com/anti-money-laundering-ai/sla?hl=en)	Apigee (https://cloud.google.com/apigee/sla?hl=en)
App Engine (https://cloud.google.com/appengine/sla?hl=en)	Application Integration (https://cloud.google.com/application-integration/sla?hl=en)
AutoML Translation (https://cloud.google.com/translate/automl/sla?hl=en)	Bare Metal Solution (https://cloud.google.com/bare-metal/sla?hl=en)
BigQuery (https://cloud.google.com/bigquery/sla?hl=en)	Blockchain Node Engine (https://cloud.google.com/blockchain-node-engine/sla?hl=en)
Certificate Authority Service (https://cloud.google.com/certificate-authority-service/sla?hl=en)	Cloud Bigtable (https://cloud.google.com/bigtable/sla?hl=en)
Cloud CDN (https://cloud.google.com/cdn/sla?hl=en)	Cloud Build (https://cloud.google.com/build/sla?hl=en)
Cloud Data Fusion (https://cloud.google.com/data-fusion/sla?hl=en)	Cloud Composer (https://cloud.google.com/composer/sla?hl=en)
Cloud DNS (https://cloud.google.com/dns/sla?hl=en)	Cloud DLP (https://cloud.google.com/sensitive-data-protection/sla)
Cloud External Key Manager (https://cloud.google.com/ekm/sla?hl=en)	Cloud Healthcare (https://cloud.google.com/healthcare/sla?hl=en)
Cloud HSM (https://cloud.google.com/kms/sla?hl=en)	Cloud Identity Services (https://cloud.google.com/terms/identity/sla?hl=en)

Cloud Interconnect (https://cloud.google.com/network-connectivity/docs/interconnect/sla?hl=en)	Cloud Key Management Service (https://cloud.google.com/kms/sla?hl=en)
Cloud Natural Language API (https://cloud.google.com/natural-language/sla?hl=en)	Cloud NAT (https://cloud.google.com/nat/sla?hl=en)
Cloud NGFW (https://cloud.google.com/firewall/sla?hl=en)	Cloud Observability (Monitoring, Logging) (https://cloud.google.com/operations/sla)
Cloud Run (https://cloud.google.com/run/sla?hl=en)	Cloud Run functions (https://cloud.google.com/functions/sla?hl=en)
Dataproc (https://cloud.google.com/dataproc/sla?hl=en)	Datastore (https://cloud.google.com/datastore/sla?hl=en)
Cloud Scheduler (https://cloud.google.com/scheduler/sla?hl=en)	Cloud Service Mesh (https://cloud.google.com/terms/service-mesh/sla?hl=en)
Cloud Spanner (https://cloud.google.com/spanner/sla?hl=en)	Cloud SQL (https://cloud.google.com/sql/sla)
Cloud Storage (https://cloud.google.com/storage/sla?hl=en)	Cloud Storage for Firebase (https://firebase.google.com/terms/service-level-agreement/cloud-storage)
Cloud Tasks (https://cloud.google.com/tasks/sla)	Cloud Translation (https://cloud.google.com/translate/sla?hl=en)
Cloud Vision (https://cloud.google.com/vision/sla?hl=en)	Cloud VPN (https://cloud.google.com/network-connectivity/docs/vpn/sla?hl=en)
Cloud Workstations (https://cloud.google.com/workstations/sla)	Compute Engine and Load Balancing (https://cloud.google.com/compute/sla?hl=en)
Dataflow (https://cloud.google.com/dataflow/sla?hl=en)	Dataplex (https://cloud.google.com/dataplex/sla?hl=en)
Dataproc Metastore	Data Catalog

(https://cloud.google.com/dataproc-meta-store/sla?hl=en)	(https://cloud.google.com/data-catalog/sla?hl=en)
Dialogflow (https://cloud.google.com/dialogflow/sla?hl=en)	Document AI (https://cloud.google.com/document-ai/sla?hl=en)
Filestore (https://cloud.google.com/filestore/sla?hl=en)	Firebase Data Connect (https://cloud.google.com/terms/sla/firebase-data-connect?hl=en)
Firestore (https://cloud.google.com/firestore/sla?hl=en)	Gemini Enterprise (https://cloud.google.com/terms/gemini-enterprise/sla?hl=en)
Gemini for Google Cloud (https://cloud.google.com/products/gemini/sla?hl=en)	Gemini on Vertex (https://cloud.google.com/vertex-ai/generative-ai/sla?hl=en)
Google Cloud Armor (https://cloud.google.com/armor/sla?hl=en)	Google Cloud Contact Center as a Service (CCaaS) (https://cloud.google.com/terms/contact-center/ccai-platform/sla?hl=en)
Google Cloud NetApp Volumes (https://cloud.google.com/netapp/volumes/sla?hl=en)	Google Cloud VMware Engine (https://cloud.google.com/vmware-engine/sla?hl=en)
Google Earth Engine (https://cloud.google.com/earth-engine/sla?hl=en)	Memorystore (https://cloud.google.com/memorystore/sla?hl=en)
Network Connectivity Center (https://cloud.google.com/ncc/sla?hl=en)	Google Kubernetes Engine (https://cloud.google.com/kubernetes-engine/sla?hl=en)
Identity Platform (https://cloud.google.com/identity-platform/sla?hl=en)	IoT Core (https://docs.cloud.google.com/architecture/connected-devices/iot-platform-product-architecture)
Looker (Google Cloud core) (https://cloud.google.com/terms/looker-core/sla?hl=en)	Looker Studio Pro (https://cloud.google.com/looker-studio/sla?hl=en)
Managed Service for Apache Kafka (https://cloud.google.com/terms/managed-service-for-apache-kafka/sla?hl=en)	Managed Service for Microsoft Active Directory (https://cloud.google.com/managed-microsoft-ad/sla?hl=en)
Media CDN	Parallelstore

(https://cloud.google.com/media-cdn/sla)	(https://cloud.google.com/terms/parallel-store/sla?hl=en)
Pub/Sub (https://cloud.google.com/pubsub/sla?hl=en)	reCAPTCHA Enterprise (https://cloud.google.com/recaptcha/sla)
Secret Manager (https://cloud.google.com/secret-manager/sla?hl=en)	Secure Web Proxy (https://cloud.google.com/terms/secure-web-proxy/sla?hl=en)
Security Command Center (https://cloud.google.com/security-command-center/sla?hl=en)	Spectrum Access System (https://cloud.google.com/sas/sla?hl=en)
Speech-to-Text (https://cloud.google.com/speech-to-text/sla?hl=en)	Talent Solution (https://cloud.google.com/talent-solution/sla?hl=en)
Text-to-Speech (https://cloud.google.com/text-to-speech/sla?hl=en)	Transcoder API (https://cloud.google.com/terms/transcoder/sla?hl=en)
Vertex AI Feature Store (https://cloud.google.com/terms/vertex-ai/featurestore/sla?hl=en)	Vertex AI Platform (https://cloud.google.com/vertex-ai/sla?hl=en)
Vertex AI Search for commerce (https://cloud.google.com/retail/sla?hl=en)	Vertex AI Vector Search (https://cloud.google.com/terms/vector-search/sla?hl=en)
Vertex AI Vision (https://cloud.google.com/vertex-ai-vision/sla?hl=en)	Video Intelligence API (https://cloud.google.com/video-intelligence/sla?hl=en)
Workflows (https://cloud.google.com/workflows/sla?hl=en)	



SecOps Service Level Agreements

The following are the Service Level Agreements for the following SecOps Services.

Google SecOps - SIEM

Google SecOps - SOAR

Mandiant Offerings

Google Threat Intelligence and VirusTotal

Previous versions (Last modified October 30, 2024)

September 12 2024

Google SecOps - SIEM Service Level Agreement

During the Term of the agreement under which Google has agreed to provide Google SecOps - SIEM to Customer (the "Agreement"), the Covered Service will provide a Monthly Uptime Percentage to Customer of at least 99% (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 SecOps - SIEM under a 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.

- "Covered Service" means Google SecOps - SIEM, excluding any Pre-GA Offerings, proof-of-concept or unpaid trials of Google SecOps - SIEM.
- "Downtime" means with respect to the Covered Service: the Customer is not able to access the user interface or all APIs.
- "Downtime Period" means with respect to the Covered Service: five consecutive minutes of Downtime. Intermittent Downtime for a period of less than five minutes will not be counted towards any Downtime Period. Downtime as part of Scheduled Maintenance will not be counted towards any Downtime Period.
- "Financial Credit" means the following for the Covered Service (except as otherwise set forth below):

Monthly Uptime Percentage	Percentage of monthly bill (or prorated on a monthly basis if billing is not monthly) for the Covered Services which did not meet SLO that will be credited to future bills of Customer
95%–< 99%	3%
90%–< 95%	10%
<90%	15%

- "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.
- "Scheduled Maintenance" is Downtime related to network, hardware, or software maintenance or upgrades. Scheduled Maintenance will be performed at Google's discretion.

Customer Must Request Financial Credit

In order to receive any of the Financial Credits described above, Customer must notify Google Technical Support (https://support.google.com/cloud/contact/cloud_platform_sla) within 30 days from the time Customer becomes eligible to receive a Financial Credit with a complete description of the Downtime and for how long. 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 annual billing cycle will not exceed 7% of the amount due by Customer for the applicable Covered



Service for the applicable annual cycle. Financial Credits will be made in the form of a monetary credit applied to future use of the Covered Service.

SLA Exclusions

The SLA does not apply to any: (a) features or Services designated alpha or beta (unless otherwise set forth in the associated Documentation), (b) features or Services excluded from the SLA (in the associated documentation), (c) features or Services that have been deprecated, (d) inability to utilize the Services due to Customer not having transferred usable Customer Data to the Services, or (e) 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, regardless of whether Google suggested or otherwise supported Customer's use of the hardware or software; (iii) that resulted from abuses or other behaviors that violate the Agreement; or (iv) that resulted from quotas applied by the Services or listed in the Agreement or documentation.

Previous versions (*Last modified October 30, 2024*)
February 6 2024, October 24 2022, October 1 2020

Google SecOps - SOAR Service Level Agreement

During the Term of the Agreement under which Google has agreed to provide Google SecOps - SOAR to Customer (the "Agreement"), the Covered Service will provide a Monthly Uptime Percentage to Customer of at least 99% (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 SecOps - SOAR under a 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.

- "Covered Service" means Google SecOps - SOAR, excluding any Pre-GA Offerings, proof-of-concept or unpaid trials of Google SecOps - SOAR.
- "Downtime" means with respect to the Covered Service: the Customer is not able to access the user interface or all APIs.
- "Downtime Period" means with respect to the Covered Service: five consecutive minutes of Downtime. Intermittent Downtime for a period of less than five minutes will not be counted towards any Downtime Period. Downtime as part of Scheduled Maintenance will not be counted towards any Downtime Period.

- "Financial Credit" means the following for the Covered Service (except as otherwise set forth below):

Monthly Uptime Percentage	Percentage of monthly bill (or prorated on a monthly basis if billing is not monthly) for the Covered Services which did not meet SLO that will be credited to future bills of Customer
95%–< 99%	3%
90%–< 95%	10%
<90%	15%

- "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.
- "Scheduled Maintenance" is Downtime related to network, hardware, or software maintenance or upgrades. Scheduled Maintenance will be performed at Google's discretion.

Customer Must Request Financial Credit

In order to receive any of the Financial Credits described above, Customer must notify Google technical support (https://support.google.com/cloud/contact/cloud_platform_sla) within 30 days from the time Customer becomes eligible to receive a Financial Credit with a complete description of the Downtime and for how long. 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 annual billing cycle will not exceed 7% of the amount due by Customer for the applicable Covered Service for the applicable annual cycle. Financial Credits will be made in the form of a monetary credit applied to future use of the Covered Service.

SLA Exclusions

The SLA does not apply to any: (a) features or Services designated alpha or beta (unless otherwise set forth in the associated Documentation), (b) features or Services excluded from the SLA (in the associated documentation), (c) features or Services that have been deprecated, (d) inability to utilize the Services due to Customer not having transferred usable Customer Data to the Services, or (e) 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, regardless of whether Google suggested or otherwise supported Customer's use of the hardware or software; (iii) that resulted from abuses or other behaviors that violate the Agreement; or (iv) that resulted from quotas applied by the Services or listed in the Agreement or documentation.

Previous versions (*Last modified October 30, 2024*)
February 6 2023, November 1 2022

Mandiant Offerings Service Level Agreement

During the Term of the agreement under which Google has agreed to provide Mandiant Managed Defense Portal, Mandiant Threat Intelligence Portal, Mandiant Security Validation Portal, and Mandiant Attack Surface Management Portal, Google will provide the service levels and service credits specified below.

Uptime

With respect to the Managed Defense Portal, Google will undertake commercially reasonable efforts to ensure portal availability for 99.9% of the time during each calendar month.

With respect to the Mandiant Threat Intelligence Portal, Mandiant Security Validation Portal, and the Mandiant Attack Surface Management Portal, Google will undertake commercially reasonable efforts to ensure portal availability for 99.5% of the time during each calendar month.

- "Service Outage" means the portal is not available due to a failure or a disruption in the portal that is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or the act or omission of Customer.
- "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the portal may be performed.
- "Emergency Maintenance" means any time outside of Scheduled Maintenance that Google requires to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required,



Google will notify Customer, to the extent possible under the circumstances, and provide the expected time frame of the Emergency Maintenance and availability of the portal during the Emergency Maintenance.

- "System Availability" means the number of minutes in any calendar month minus the aggregate number of minutes of all Service Outages that occur during that calendar month.

Remedy

If the portal does not meet the monthly service availability defined above, Google will provide a credit to the Customer in accordance with the table below ("Credit") for a validated Service Level Claim (defined below). The percentage of portal availability per calendar month (in the table below) is equal to the result, expressed as a percentage, of the number of minutes of System Availability in a calendar month divided by the total number of minutes in the calendar month.

Percent of Portal Availability per Calendar Month	Service Credit
<99.9% (Managed Defense Portal) <99.5% (Mandiant Threat Intelligence Portal) <99.5% (Mandiant Security Validation Portal) <99.5% (Mandiant Attack Surface Management Portal)	2%
<99.0%	5%
<98.0%	10%

- For determining the Credit, the duration of a Service Outage will be measured as the time starting when Customer experiences a disruption in availability of the portal and ending when a successful solution or workaround allowing for full restoration of the portal is provided by Google to Customer. Customer



must notify Google of any Service Outage and request a Credit in writing no later than fifteen (15) days after the calendar month in which the Service Outage occurred ("Service Level Claim") to be entitled to a Credit for that Service Outage.

- Any Credits earned by Customer hereunder will be applied to the Fees owed by Customer for the next Order Term for which the Credit applies. If Credits cannot be applied to future Fees because the Order Term has terminated for non-renewal or for a material uncured breach, or termination for convenience, by Customer, such Credits will become null and void. If Credits cannot be applied to future Fees because the Order Term has terminated due to a material uncured breach by Google, Google will promptly pay Customer the amount of the Credit.
- Customer will not be entitled to receive a Credit that exceeds 10% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

Google Threat Intelligence ("GTI")/VirusTotal ("VT") Service Level Agreement

During the Term of the Agreement under which Google has agreed to provide GTI/VT to Customer (the "Agreement"), the the GTI/VT web interface and the API ("Covered Service") currently located at www.virustotal.com, or a successor thereto, will be operational and available to Customer at least 99.9% of the time in any calendar month (the "SLA").

If Google does not meet the SLA, and if Customer meets its obligations under this SLA, Customer will be eligible to receive the Service Credits described below. This SLA states Customer's sole and exclusive remedy for any failure by Google to meet the SLA. 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 GTI/VT under a partner or reseller program, then all references to Customer in this SLA mean Partner or Reseller (as applicable), and any Service Credit(s) will only apply for impacted Partner or Reseller order(s) under the Agreement.

Definitions

The following definitions apply to the SLA:

- "Downtime" means the amount of time, measured in minutes, that a Covered Service is returning an HTTP 5XX error code to the Customer in a calendar month, provided such amount of time is in consecutive periods of at least five minutes.
- "Service Credit" means the following:

--	--

Percentage of Downtime per calendar month	Service Credit expressed as calendar days of Covered Service added to the term end of the Agreement, at no charge to Customer
> 5%	30
>1% and <= 5%	10
>.1% and <= 1%	5

Customer Must Request Service Credit

In order to receive any of the Service Credits described above, Customer must notify Google at contact@virustotal.com within 30 calendar days from the time Customer becomes eligible to receive a Service Credit. Failure to comply with this requirement will forfeit Customer's right to receive a Service Credit.

Maximum Service Credit

The aggregate maximum number of Service Credits that Google will issue to Customer for all Downtime that occurs in a single calendar month will not exceed 30 calendar days of Covered Service added to the end of Customer's term for the Covered Service. Service Credits may not be exchanged for or converted to monetary amounts or transferred to another party.

Exclusions

The SLA does not apply to any Covered Service that expressly excludes this SLA (as stated in the documentation for such Covered Service), free Services (e.g., free users, introductory trial periods, etc) or any performance issues: (a) caused by factors outside Google's reasonable control; or (b) that resulted from Customer's equipment or third party equipment, or both (not within the primary control of Google).



Other support

Google will provide reasonable support to Customer for technical or operational issues related to the Covered Service. Google will use commercially reasonable efforts to reply to Customer's written inquiry within 2 business days of Google's receipt of Customer's request.



Google Workspace Service Level Agreement

Last modified: January 30, 2025

Google Workspace SLA. During the Term of the agreement under which Google has agreed to provide the applicable Covered Services to Customer (as applicable, the "Agreement"), the Monthly Uptime Percentage will be at least 99.9% in any calendar month (the "Google Workspace SLA"). If Google does not meet the Google Workspace SLA, and if Customer complies with the requirements under this Google Workspace SLA, Customer will be eligible to receive the Service Credits described below. This Google Workspace SLA states Customer's sole and exclusive remedy for any failure by Google to meet the Google Workspace SLA.

Definitions. The following definitions shall apply to the Google Workspace SLA.

"Downtime" means, for a domain, a period of time during which the user web interface for the applicable Covered Services used by Customer has more than a five percent user error rate.

Downtime is measured based on server side error rate.

"AppSheet Covered Services" means the AppSheet Enterprise Standard and AppSheet Enterprise Plus versions of AppSheet.

"Covered Services" means AppSheet Covered Services or Google Workspace Covered Services, as applicable.

"Google Workspace Covered Services" means the Gmail, Google Calendar, Google Chat, Google Cloud Search, Google Docs, Google Drive, Google Forms, Google Groups for Business, Google Keep, Google Meet, Google Sheets, Google Sites, Google Slides, Google Tasks, Google Vault, Google Vids, and Google Voice components of the Services, excluding Gmail Labs functionality.

"Monthly Uptime Percentage" means total number of minutes in a calendar month minus the number of minutes of Downtime in a calendar month, divided by the total number of minutes in a calendar month.

"Service" means the Google Workspace Services.

"Service Credit" means the following:

Monthly Uptime Percentage	Days of Service added to the end of the Service term (for offline billing customers), or monetary credit equal to the value of days applied to a future invoice (for online billing customers), for the applicable Covered Service(s) that did not meet the Google Workspace SLA
< 99.9% - >= 99.0%	3

< 99.0% - >= 95.0%	7
< 95.0%	15

Customer Must Request Service Credit. In order to receive any of the Service Credits described above, Customer must notify Google (or, if Customer ordered Services from a Reseller, Customer must notify Customer's Reseller who must notify Google) by creating a support case within thirty days from the time Customer becomes eligible to receive a Service Credit. Failure to comply with this requirement will forfeit Customer's right to receive a Service Credit. If Customer ordered Services from a Reseller and complies with this requirement, Customer will receive the applicable Service Credit from Customer's Reseller on behalf of Google.

Maximum Service Credit. The aggregate maximum number of Service Credits to be issued by Google (or, if Customer ordered Services from a Reseller, by Customer's Reseller on behalf of Google) to Customer for all Downtime that occurs in a single calendar month for the applicable Covered Service shall not exceed fifteen days of Service added to the end of Customer's term for that Covered Service (or the value of 15 days of Service in the form of a monetary credit if Customer is billed monthly). Service Credits may not be exchanged for, or converted to, monetary amounts, except where Customer purchased online and is billed monthly, in which case Google will apply an equivalent credit on a future invoice for Customer.

Google Workspace Essentials Service Credit. If Customer orders Google Workspace Essentials edition directly from Google, any Service Credits that may be due to Customer will be issued in the form of monetary credits (and not additional Service days) that will be applied to Customer's next invoice. If Customer orders Google Workspace Essentials edition from a Reseller, Google will issue to Customer's Reseller any Service Credits that may be due to Customer in the form of monetary credits (and not additional Service days).

Google Workspace SLA Exclusions. This Google Workspace SLA does not apply to (i) any services that expressly exclude it (as stated in the documentation for such services), (ii) any services comprised within the Google Workspace Essentials Starter edition (notwithstanding that this SLA may define such services as Google Workspace Covered Services), or (iii) any performance issues: (a) caused by factors described in the "Force Majeure" section of the Agreement; (b) that resulted from Customer's equipment and/or third party equipment, (not within the primary control of Google); or (c) that resulted from Customer's or its End Users' abuses or other behaviors that violate the Agreement.

Previous Versions

Last modified January 30, 2025

November 7, 2024



June 17, 2024
November 15, 2023
August 14, 2023
January 11, 2023
July 12, 2021
December 21, 2020
December 9, 2020



Google's Looker (original) Service Level Agreement (SLA) for Looker Hosted Deployments

During the Term of the agreement under which Google has agreed to provide the Covered Services to Customer (as applicable, the "Agreement"), the Covered Services will be Available to Customer as described below (the "Service Level Objective" or "SLO"). Capitalized terms used in this SLA, but not defined in this SLA, have the meanings given to them in the Agreement.

Looker (original) Platform: Each Looker (original) Platform will include a Service Level Objective as follows:

Looker (original) Platform	Monthly Uptime Percentage the Covered Service will be Available (SLO)
Standard	>= 99.5%
Advanced or Elite	>= 99.9%

- **SLO Exclusions.** The SLO does not apply to any of the following: (a) Customer's environment or use of the Covered Services not consistent with the Documentation or as described in the Agreement, (b) Maintenance performed, including update/upgrade releases for the Services, (c) any unavailability caused by circumstances or events outside Google's reasonable control, including any force majeure event, internet access, Customer's or any third party's actions or inactions, equipment, software, or other technology, (d) Instances provisioned for development, staging or other non-production usage, or (e) a Suspension or remedial action described in the Agreement.
- **Availability.** In the event the Covered Services do not meet the applicable SLO, and if Customer meets its obligations under this SLA, Customer will be eligible to receive a Service Credit. This SLA states Customer's sole and exclusive remedy for any failure by Google to meet the applicable SLO.
- **Service Credit Calculation.** The Service Credit is calculated as a percentage of Customer's Monthly Fee. Service Credits will apply only against future payments due from Customer. A Service Credit awarded in any calendar



month shall not, under any circumstances, exceed the Monthly Fee paid by Customer.

- **Service Credit Request Requirement.** Customer must provide all reasonable details regarding the claim, including but not limited to, a detailed description of the incident, the duration of the incident, the number of affected End Users, and any attempts made by Customer to resolve the incident. Customer must submit a request by completing the form at the following link: https://support.google.com/cloud/contact/looker_sla by the end of the month following the month in which the incident occurred. If Customer is past due with respect to any payment or in default with respect to any material contractual obligations to Google, then Customer is not eligible for any Service Credit under this SLA. Google shall review and grant requests for Services Credits by using Google's system logs and other records, which shall be considered definitive.

SLA Definitions

- "Available" means that the Covered Services can be accessed by End Users.
- "Covered Services" means Looker Hosted Deployment Services.
- "End User Fee" means the average number of End Users subscribed on the affected Instance during the month in which the Covered Services did not meet the applicable SLO multiplied by the monthly per End User fee, as specified in the applicable Order Form.
- "Maintenance" means maintenance work that is performed on hardware or software delivering the Services.
- "Monthly Fee" means the Platform Fee plus the End User Fee.
- "Platform Fee" means the total Platform fee, as specified in the applicable Order Form, paid by Customer for the affected Instance divided by the total number of months in the Term.
- "Service Credit" means the following for each of the respective Looker (original) Platforms:

Standard Platform Platform

Monthly Uptime Percentage Standard Platform	Service Credit Percentage
99.0% <= 99.5%	10%

< 99%	25%
Advanced or Elite Platform	
Monthly Uptime Percentage Advanced or Elite	Service Credit Percentage
99.0% <= 99.9%	10%
< 99%	25%

Previous versions (Last modified May 8, 2023)

May 5 2022, April 1 2021, June 1 2020, March 9 2020



Google Cloud Services: Technical Support Services Guidelines

For translations of these Technical Support Services Guidelines into other languages, please click on the appropriate link: Bahasa Indonesia (<https://services.google.com/fh/files/misc/id-cloud-technical-support-services-guidelines.pdf>), Deutsch (<https://services.google.com/fh/files/misc/de-cloud-technical-support-services-guidelines.pdf>), Español (Latinoamérica) (<https://services.google.com/fh/files/misc/es-419-cloud-technical-support-services-guidelines.pdf>), Français (<https://services.google.com/fh/files/misc/fr-cloud-technical-support-services-guidelines.pdf>), Italiano (<https://services.google.com/fh/files/misc/it-cloud-technical-support-services-guidelines.pdf>), Nederlands (<https://services.google.com/fh/files/misc/nl-cloud-technical-support-services-guidelines.pdf>), Português (<https://services.google.com/fh/files/misc/pt-br-cloud-technical-support-services-guidelines.pdf>), 한국어 (<https://services.google.com/fh/files/misc/ko-cloud-technical-support-services-guidelines.pdf>), 日本語 (<https://services.google.com/fh/files/misc/ja-cloud-technical-support-services-guidelines.pdf>)

These technical support services guidelines (“Guidelines”) are incorporated into the agreement under which Google has agreed to provide Google Cloud Platform and SecOps Services (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. Google does not provide Technical Support Services (“TSS”) for certain Google Cloud Platform Services and SecOps Services, and some Google Cloud Platform Services, SecOps Services and related products are subject to additional or different technical support terms as noted in the General Support Services Terms: Exceptions section.

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.* 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.*

a. *Pre-GA Offerings.* Google has no obligation to provide TSS for Pre-GA Offerings (as defined in the Service Specific Terms) or any offerings identified as "Preview," "Alpha," "Beta," "Experimental," or similar designation, but will consider Requests relating to Pre-GA Offerings or similar offerings on a case-by-case basis.

b. *Pre-GA Support Offerings Terms.* Google may make available to Customer pre-general availability technical support services or features, in each case, that are identified as "Preview," "Alpha," "Beta," "Experimental," or similar designation in related documentation or materials or are not yet listed in these Guidelines (collectively, "Pre-GA Support Offerings"). While Pre-GA Support Offerings are not TSS, Customer's use of Pre-GA Support Offerings is subject to the terms of these Guidelines, as amended by this Section (Pre-GA Support Offerings Terms) and, any



additional terms provided to Customer in the Google Support Tool or order form or otherwise presented by Google (the "Additional Pre-GA Support Terms"). In the event of conflict between the terms of these Guidelines and the Additional Pre-GA Support Terms, the Additional Pre-GA Support Terms govern.

1. Pre-GA Support Offerings may be changed, suspended, or discontinued at any time without prior notice to Customer.

2. At its option, Customer may provide feedback and suggestions about the Pre-GA Support Offerings to Google ("Pre-GA Support Feedback"). If Customer provides Pre-GA Support Feedback, then Google and its Affiliates may use that Pre-GA Support Feedback without restriction and without obligation to Customer, excluding any Pre-GA Support Feedback marked as Customer Confidential Information.

3. Target initial response times and language support as described in these Guidelines may be different or unavailable for Pre-GA Support Offerings.

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. **Technical Account Management (TAM).** As part of the Platinum, Enterprise and Premium Support offerings, Customer will receive access to Technical Account Management services 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.

8. 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.

9. 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 technology partners who have collaborated with Google to offer technologies that can be used in conjunction with the Services (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 or communicate with the Collaborative Support Partner on Customer's behalf, subject to the following terms:

9.1. 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.

9.2. Google will include Collaborative Support Partners in direct support communications with Customer, or communicate with the Collaborative Support Partner on Customer's behalf, solely at Customer's direction and only after receiving Customer's consent.

9.3. When Customer consents to involve a Collaborative Support Partner in an ongoing support case:

- a. Customer consents to Google providing that Collaborative Support Partner with information Google reasonably deems relevant to the Request, including Customer's name, contact information, and a description of the Request;
- b. the Collaborative Support Partner acts as an independent contractor of the Customer, not Google; and
- c. the Collaborative Support Partner, not Google, is solely responsible for the processing and use of any information provided to that Collaborative Support Partner in the course of providing support services.

10. 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:



10.1. 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;

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

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

11. 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.

12. Exceptions. Regardless of any other statement in the Agreement or these Guidelines, Google does not offer TSS for Looker Studio (except for Looker Studio Pro), Mandiant Managed Services, Mandiant Consulting Services, Expertise on Demand, SecOps Training Services, and Security Customer Success Services. Google will provide Comprehensive Support for Looker (Google Cloud core) and Google Threat Intelligence as described at <https://cloud.google.com/terms/tssg/comprehensive>.

For the following Google Cloud Platform and SecOps Services, Google offers technical support under separate terms set forth at the corresponding URL:

Service	Technical Support Terms
Cloud Identity	https://cloud.google.com/terms/identity/tssg
Apigee Edge **	https://cloud.google.com/terms/apigee-support ("Apigee Edge TSSG")
VirusTotal	https://www.virustotal.com/gui/contact-us/technical-support

For the following Google Cloud Platform Services and related products, Google offers TSS under these Guidelines except as provided at the corresponding URL:

Service/Product	Technical Support Terms
-----------------	-------------------------

Looker (original)	https://cloud.google.com/terms/tssg/looker
Firebase	https://cloud.google.com/terms/tssg/firebase
Apigee, Apigee Edge**	https://cloud.google.com/terms/apigee-support-services-guide ("Apigee Support Services Guide")
Google Cloud Backup and DR	https://cloud.google.com/terms/gcldr-services-guide

**TSS for legacy Apigee Edge customers who have not yet renewed Apigee Edge to have their support provided by these TSS (as modified by the Apigee Support Services Guide) will be provided under the Apigee Edge TSSG. All other Apigee Edge customers will have TSS provided under these TSS (as modified by the Apigee Support Services Guide).

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

13.9. "*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.

13.10. "*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 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.
- 13.22. *"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. Chrome Frame is a separate product not covered under these Guidelines.
- 13.23. *"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 and Partner-led Enhanced Support

In this Section (Enhanced Support and Partner-led Enhanced Support), for Partner-led Enhanced Support, each reference to 'Customer' means 'Partner' or 'Reseller' (as applicable).

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. Customer must maintain a concurrent subscription to Enhanced Support during the applicable order term for each Value Add Service:

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 (a) English, (b) Hebrew for Assured Workloads in the Israel-only region, and (c) Japanese for Assured Workloads in the Japan-only region only. Such regions are described in the applicable documentation for Assured Workloads.

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. Data Boundary by Partners Support for Enhanced Support. If (i) Customer is using Data Boundary by Partners; and (ii) Customer has purchased Enhanced Support, then Google will provide TSS for the In-scope Google Cloud Controls defined at <https://cloud.google.com/terms/in-scope-sovereign-cloud> (“Data Boundary by Partners Support”) in accordance with the Customer-selected security controls in the Admin Console. All Requests for Data Boundary 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 Data Boundary by Partners Project with the relevant Data Boundary Partner. Google will provide Data Boundary by Partners Support in the English language only.

1.2.5. Live Event Support for CDN for Enhanced Support. If Customer plans to host a live event using a Google Cloud Platform CDN Service (“Live Event”), and Customer wishes to purchase Live Event Support for such event, it must do so no less than 30 days before that Live Event to ensure proper planning. Prior to each Live Event, Google and Customer will agree and document a plan that includes requirements gathering, architecture review, data thresholds, and identification of Customer’s and Google’s designated points of contact. During the Live Event, Google will provide Customer with access to a video conference bridge with Google Support Personnel. Each Live Event is limited to 5 hrs. During each Live Event, Google will create P1 support cases on behalf of Customer in lieu of Customer submitting a Request. Regardless of Section 2 (Target Initial Response Times for Enhanced Support) below, Google will respond to such support cases with a target initial response time of 5 minutes after case creation. There is no limit on the number of Live Events that Customer may purchase per calendar year. Google Support Personnel will provide support in the English language only.

1.2.6. Monitoring as a Service (MaaS) for Enhanced Support. If Customer wishes to purchase MaaS it must do so no less than 30 days prior to the start of the requested monitoring period. Prior to the monitoring period, Google and Customer will agree and document selected criteria for proactive alerting. Google will provide proactive monitoring of the agreed upon alerting thresholds of the Customer’s applicable Service deployment. Google will automatically create P1 support cases based on the agreed upon alerting thresholds in lieu of Customer submitting a Request. Regardless of Section 2 (Target Initial Response Times for Enhanced Support) below, Google will respond to such support cases with a target initial response time of 5 minutes after case creation. Google Support Personnel will provide support in the English language only.

2. Partner-led Enhanced Support.

2.1. Partner-led Enhanced Support includes unlimited Designated Contacts.

2.2. Value Add Services. Customers may purchase the following Value Add Services for an additional fee. Customers must maintain a concurrent subscription to Partner-led Enhanced Support during the applicable order term for each Value Add Service:

2.2.1 Partner Operations Management Service (POMs). Partner Operations Management Service (POMS) is available as a Value Add Service with Partner-led Enhanced Support. POMs includes: (a) assistance in developing a cloud strategy with respect to the Services, (b) best practices guidance on implementing and



executing the strategy in collaboration with Google Cloud Support, and (c) management of technical support escalations and coordination with Google subject matter experts to address technical inquiries related to the Services. Additional access to Partner Operations Management Service may be purchased, subject to additional fees and terms. Any additional access or continued access to Partner Operations Management Service requires that Customer maintain a concurrent subscription to Partner-led Enhanced Support, as applicable.

3. 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

4. Enrollment and Unenrollment of Enhanced Support and Partner-led Enhanced Support.

4.1. Enhanced Support and Partner-led Enhanced Support each require a minimum commitment as described in the applicable Order Form.

4.2. Customer may unenroll from Enhanced Support or Partner-led 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, Partner-led Premium Support, and Tech Partner Premium Support

In this Section (Premium Support, Partner-led Premium Support and Tech Partner Premium Support), for Partner-led Premium Support, each reference to 'Customer' means 'Partner' or 'Reseller' (as applicable).

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 7 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. Customer must maintain a concurrent subscription to Premium Support during the applicable order term for each Value Add Service:

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 (a) English, (b) Hebrew for Assured Workloads in the Israel-only region and (c) Japanese for Assured Workloads in the Japan-only-region only. Such regions are described in the applicable documentation for Assured Workloads.

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. *Data Boundary by Partners Support for Premium Support*. If (i) Customer is using Data Boundary by Partners; and (ii) Customer has purchased Premium Support, then Google will provide TSS for the In-scope Google Cloud Controls defined at <https://cloud.google.com/terms/in-scope-sovereign-cloud> ("Data Boundary by Partners Support") in accordance with the Customer-selected security controls in the Admin Console. All Requests for Data Boundary 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 Data Boundary by Partners Project with the relevant Data Boundary Partner. Google will provide Data Boundary by Partners Support in the English language only.

1.3.4. *Live Event Support for CDN for Premium Support*. If Customer plans to host a live event using a Google Cloud Platform CDN Service ("Live Event"), and Customer wishes to purchase Live Event Support for such event, it must do so no less than 30 days before that Live Event to ensure proper planning. Prior to each Live Event, Google and Customer will agree and document a plan that includes requirements gathering, architecture review, data thresholds, and identification of Customer's and Google's designated points of contact. During the Live Event, Google will provide Customer with access to a video conference bridge with Google Support Personnel. Each Live Event is limited to 5 hrs. During each Live Event, Google will create P1 support cases on behalf of Customer in lieu of Customer submitting a Request. Regardless of Section 3 (Target Initial Response Times for Premium Support, Partner-led Premium Support and Tech Partner Premium Support) below, Google will respond to such support cases with a target initial response time of 5 minutes after case creation. There is no limit on the number of Live Events that Customer may purchase per calendar year. Google Support Personnel will provide support in the English language only.



1.3.5. Monitoring as a Service (MaaS) for Premium Support. If Customer wishes to purchase MaaS it must do so no less than 30 days prior to the start of the requested monitoring period. Prior to the monitoring period, Google and Customer will agree and document selected criteria for proactive alerting. Google will provide proactive monitoring of the agreed upon alerting thresholds of the Customer's applicable Service deployment. Google will automatically create P1 support cases based on the agreed upon alerting thresholds in lieu of Customer submitting a Request. Regardless of Section 3 (Target Initial Response Times for Premium Support, Partner-led Premium Support and Tech Partner Premium Support) below, Google will respond to such support cases with a target initial response time of 5 minutes after case creation. Google Support Personnel will provide support in the English language only.

2. Partner-led Premium Support and Tech Partner Premium Support.

2.1. Partner-led Premium Support and Tech Partner Premium Support includes unlimited Designated Contacts.

2.2. Partner Operations Management Service (POMs). As part of the Partner-led Premium Support and Tech Partner Premium Support offerings, Customer will receive access to the Partner Operations Management Service (POMS). POMs includes: (a) assistance in developing a cloud strategy with respect to the Services, (b) best practices guidance on implementing and executing the strategy in collaboration with Google Cloud Support, and (c) management of technical support escalations and coordination with Google subject matter experts to address technical inquiries related to the Services. Additional access to Partner Operations Management Service may be purchased, subject to additional fees and terms. Any additional access or continued access to Partner Operations Management Service requires that Customer maintain a concurrent subscription to Partner-led Premium Support or Tech Partner Premium Support, as applicable.

3. Target Initial Response Times for Premium Support, Partner-led Premium Support and Tech Partner Premium Support.

Priority	Target Initial Response Times
P0	5 minutes (Premium Support with MCS only)
P1	15 minutes
P2	2 hours
P3	4 hours*

*during the Hours of Operation

4. On-Site Support for 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, Partner-led Premium Support and Tech Partner Premium Support.

5.1. Premium Support, Partner-led Premium Support and Tech Partner Premium Support each require a minimum 1-year Fee commitment from the date on which Customer enrolls.

5.2. Customer may unenroll from Premium Support, Partner-led Premium Support or Tech Partner 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, Partner-led Premium Support, or Tech Partner 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, Partner-led Premium Support, or Tech Partner 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 7 (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	1 hours	15 minutes
P2	4 hours*	4 hours*
P3	8 hours*	8 hours*
P4	8 hours*	8 hours*

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 7 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.

Previous versions of the SecOps Services Technical Support Services Guidelines are provided below for archival purposes.

Archive versions of the Google SecOps - SIEM Technical Support Services Guidelines: October 26, 2022 and October 1, 2020

Archive versions of the Google SecOps - SOAR Technical Support Services Guidelines: August 2, 2022

Previous versions (Last modified October 13, 2025)

September 2, 2025 August 28, 2025 July 1, 2025 October 30, 2024 July 8, 2024 March 28, 2024 January 25, 2024 December 14, 2023 October 26, 2023 September 13, 2023 May 8, 2023 March 30, 2023 March 27, 2023 February 16, 2023 January

Google Cloud Terms of Service for G-Cloud 15 - Lot 1a, Lot 2a and Lot 2b (January 2026)



31, 2023 November 14, 2022 October 11, 2022 October 3, 2022 September 20, 2022 September 15, 2022 August 1, 2022 June 28, 2022 April 28, 2022 April 25, 2022 March 28, 2022 February 16, 2022 February 14, 2022 July 29, 2021 May 17, 2021 March 8, 2021 February 22, 2021 February 2, 2021 January 28, 2021 February 13, 2020 December 11, 2019 October 1, 2019 June 17, 2019 April 18, 2019 May 23, 2018 March 20, 2018 August 7, 2017



SecOps Services: Technical Support Services Guidelines

Unless otherwise stated on this page, Technical Support Services for SecOps Services are provided by Google to Customer under the Google Technical Support Services Guidelines (<https://cloud.google.com/terms/tssg>) (the "Guidelines") and as supplemented by the Comprehensive Support Guide (<https://cloud.google.com/terms/tssg/comprehensive?hl=en>) for Comprehensive Support. All references in the Guidelines to "Google Cloud Platform Services", "GCP Services", or "Services" are each deemed to be references to the SecOps Services. Capitalized terms used but not defined in the Guidelines have the meaning given to them in the Agreement.

Technical Support Services are not available for Mandiant Managed Services, Mandiant Consulting Services, Expertise on Demand, Training Services, and Security Customer Success Services.

For VirusTotal, the Technical Support Services are provided by Google to Customer at <https://www.virustotal.com/gui/contact-us/technical-support>.

Previous versions of the SecOps Services Technical Support Services Guidelines are provided below for archival purposes.

Archive versions of the Google SecOps - SIEM Technical Support Services Guidelines: October 26, 2022 (<https://cloud.google.com/terms/secops/tssg/chronicle-siem/index-20221026>) and October 1, 2020 (<https://cloud.google.com/terms/secops/tssg/chronicle-siem/index-20201001>)

Archive versions of the Google SecOps - SOAR Technical Support Services Guidelines: August 2, 2022 (<https://cloud.google.com/terms/secops/tssg/chronicle-soar/index-20220802>)



Cloud Data Processing Addendum (Customers)

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

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

General Terms

1. Overview

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

2. Definitions

2.1 In this Addendum:

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

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

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

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

3. Duration

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

4. Roles; Legal Compliance

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

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

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

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

5. Data Processing

5.1 Processor Customers. If Customer is a processor:

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

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

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

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

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

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

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

6. Data Deletion

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

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

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

7. Data Security

7.1 Google's Security Measures, Controls and Assistance.

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

7.1.2 Access and Compliance. Google will:

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

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

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

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

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

7.2 Data Incidents.

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

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

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

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

7.3 Customer's Security Responsibilities and Assessment.

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

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

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

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

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

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

7.5 Reviews and Audits of Compliance.

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

7.5.2 Customer’s Audit Rights.

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

7.5.3 Additional Business Terms for Reviews and Audits.

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

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

8. Impact Assessments and Consultations

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

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

9. Access; Data Subject Rights; Data Export

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

9.2 Data Subject Requests.

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

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

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

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

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

10. Data Processing Locations

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

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

11. Subprocessors

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

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

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

a. ensure via a written contract that:

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

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

11.4 *Opportunity to Object to Subprocessors.*

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

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

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

12. Cloud Data Protection Team; Processing Records

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

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



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

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

13. Notices

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

14. Interpretation

14.1 Precedence. To the extent of any conflict between:

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

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

Appendix 1: Subject Matter and Details of Data Processing

Subject Matter

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

Duration of the Processing

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

Nature and Purpose of the Processing

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

Categories of Data

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

Data Subjects

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

Appendix 2: Security Measures

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

1. Data Center and Network Security

(a) Data Centers.

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

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

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

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

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

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

(b) Networks and Transmission.

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

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

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



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

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

2. Access and Site Controls

(a) Site Controls.

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

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

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

(b) Access Control.

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



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

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

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

3. Data

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

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

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

4. Personnel Security

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

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

5. Subprocessor Security

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

Appendix 3: Specific Privacy Laws

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

European Data Protection Law

1. Additional Definitions.

- *"Adequate Country"* means:

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

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

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

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

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

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

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

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

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

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

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

4. Data Transfers.

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

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

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

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

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

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

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

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

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

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

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

c. in relation to Google's adoption of an Alternative Transfer Solution, at

<https://cloud.google.com/terms/alternative-transfer-solution>.

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

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

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

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

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

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

CCPA

1. Additional Definitions.

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

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

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

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

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

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

Turkey

1. Additional Definitions.

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

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

2. Data Transfers.

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

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

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

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

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

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

Israel

1. Additional Definition.

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

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

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

Brazil

1. Additional Definitions.

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

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

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

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

3. Data Transfers.

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

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

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

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

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

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

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

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

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

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

Appendix 4: Specific Products

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

Google Cloud Platform

1. Additional Definitions.

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



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

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

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

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

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

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

7. Service Specific Terms.

Bare Metal Solution (Google Cloud Platform)

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

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

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



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

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

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

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

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

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

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

Cloud NGFW (Google Cloud Platform)

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

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

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

Google Distributed Cloud connected (Google Cloud Platform)

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

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

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

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

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

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

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

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

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

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

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

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

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



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

Google-Managed Multi-Cloud (Google Cloud Platform)

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

1. Additional Definition.

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

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

Google Cloud VMware Engine (Google Cloud Platform)

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

NetApp Volumes (Google Cloud Platform)

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

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

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

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

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



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

Google Workspace and Cloud Identity

1. Additional Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

10. Service Specific Terms.

AppSheet (Google Workspace)

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

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

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

Looker (original)

1. Additional Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SecOps Services

1. Additional Definitions.

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

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

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



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

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

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

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

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

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

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

8. Service Specific Terms.

Mandiant Consulting Services and Managed Services

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

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

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



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

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

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

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

Implementation Services

1. Additional Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Google Skills for Organizations

1. Additional Definitions.

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

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

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

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

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

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

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

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

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

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

Previous versions of Data Processing and Security Terms:

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

Previous versions of Data Processing Amendment:

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

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

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

Previous versions of SecOps Services DPST (Customers):

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



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

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

Previous versions (Last modified October 23, 2025)

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

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

August 15, 2023 September 20, 2022

