



State of Oklahoma Office of Management and Enterprise Services

STATE OF OKLAHOMA AMENDMENT NO. 5 TO STATEWIDE CONTRACT AMENDMENT CONTRACT WITH CARAHSOFT TECHNOLOGY CORPORATION.

This Fifth Amendment to Oklahoma Statewide Contract No. 1041 (the “Fifth Amendment”) is effective as of the date of the last signature below, between the State of Oklahoma by and through the Office of Management and Enterprise Services and Carahsoft Technology Corporation (“Supplier”), This Fifth Amendment supplements and amends the Oklahoma Statewide Contract No. 1041 entered into by the parties and effective October 26, 2023, including all supplements and amendments thereto. Unless otherwise indicated herein, capitalized terms used in this Amendment without definition shall have the respective meanings specified in the Contract.

For good and valuable consideration, the parties agree to amend the Contract as follows:

1. Supplier and State agree the following attachment is incorporated hereto:
 - a. Attachment A: State of Oklahoma Terms and Conditions with Google, LLC
2. Attachment A shall apply to all Google products and services ordered from the Oklahoma Statewide Contract No. 1041. The parties mutually agree and understand Attachment A shall only govern as it relates to the State’s relationship with Google and shall not supersede any agreements previously made between Carahsoft and the State in relation to Oklahoma Statewide Contract No. 1041.
3. In the event of a conflict between the terms and conditions hereof and the terms and conditions of the Contract, the specific terms set forth in this Amendment shall govern the subject matter herein.
4. Except as expressly modified in this Amendment, all terms and/or provisions of the Contract not addressed herein remain as executed by the parties in the Contract and remain in full force and effect.
5. This Amendment may be executed by electronic signature in counterparts (e-mail, facsimile or otherwise). The counterparts each of which shall constitute an original, but all of which together shall constitute one and the same instrument.

Signatures

The undersigned represent and warrant that they are authorized, as representatives of the party on whose behalf they are signing, to sign this Amendment and to bind their respective party thereto:

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES:

CARAHSOFT TECHNOLOGY CORP.

By: 
Dan Cronin (Jun 26, 2025 17:37 CDT)

By: *Madeline Hall*

Name: Dan Cronin

Name: Madeline Hall

Title: State Chief Information Officer

Title: Contracts Manager

Date: 26/06/2025

Date: 6-26-25



STATE OF OKLAHOMA TERMS AND CONDITIONS WITH GOOGLE LLC

The State of Oklahoma by and through the Office of Management and Enterprise Services and Google LLC agree to the following terms for use in connection with any orders placed by the State under Oklahoma Statewide Contract No. 1041 with Carahsoft Technology Corporation for Google products and services.

These terms are effective as of the date set forth below and shall remain in effect for the duration of Oklahoma Statewide Contract No. 1041 with Carahsoft Technology Corporation, unless modified in writing by the parties.

1. The following Contract Documents are attached hereto and incorporated herein:
 - 1.1. General Terms, Attachment B;
 - 1.2. Information Technology Terms, Attachment D;
 - 1.3. Additional Terms - SecOps Services Schedule , Attachment E1;
 - 1.4. State of Oklahoma and Google LLC Agreed Information Security Requirements, Attachment E2;
 - 1.5. Google Cloud Master Agreement - Public Sector (Partner), Attachment E3;
 - 1.6. Google Cloud Master Agreement Google Cloud Platform Services Schedule; Attachment E4;
 - 1.7. Google Cloud Master Agreement Implementation Services Schedule, Attachment E5;
 - 1.8. Google Cloud Professional Services (PSO) SOW, Attachment E6; and
 - 1.9. Google Workspace Service Schedule, Attachment E7.
2. In the event of any conflicts between the terms and conditions of this Contract and its attachments, the provisions of Attachments B and D shall prevail and supersede any conflicting terms and conditions in Attachments E1 through E7.
3. The parties acknowledge and agree that the terms and conditions governing the Google Marketplace have not been reviewed, negotiated, or accepted by the State and are not contemplated under Oklahoma Statewide Contract No. 1041 with Carahsoft at this time. Supplier shall not offer or sell any products or services through Google Marketplace under Oklahoma Statewide Contract No. 1041 unless and until the terms governing such use have been negotiated and agreed to by the State in writing.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

GOOGLE LLC

By: 
Dan Cronin (Jun 25, 2025 09:45 CDT)

Name: Dan Cronin

Title: State Chief Information Officer

Date: Jun 25, 2025

By:

Name:

Title:

Date:


Philipp Schindler
Authorized Signatory

2025.06.24
09:31:34
-07'00'

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms (“General Terms”) is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

- 1.1** Supplier may not add products or services to its offerings under the Contract without the State’s prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.
- 1.2** At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory. The State’s acceptance of GCP Services may be confirmed through (1) a signed Order Form, (2) a valid Purchase Order, and (3) Google has made the GCP services available for use by the State as contracted for and intended by the parties. Acceptance of Professional Services shall be confirmed through (1) a signed Statement of Work, (2) a valid Purchase Order, and (3) notice of acceptance as described in Section 6.2 of this Attachment B.
- 1.3** If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier’s performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current Google products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an

Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.

- 1.4** The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise one (1) ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.
- 1.5** Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

- 2.1** Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.
- 2.2** Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:
 - A.** any Addendum;
 - B.** any applicable Solicitation if their incorporation into the Contract is mutually agreed to by the parties;
 - C.** any Contract-specific State terms contained in a Contract Document mutually agreed to by the parties including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;
 - D.** the terms contained in this Contract Document, including the AUP, Data Processing and Security Terms, GCP Service Specific Terms, GCP Technical Support Services Guidelines, and SLAs as defined in Attachment E4;

- E. any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;
- F. any statement of work, work order, or other similar ordering document as applicable; and
- G. other mutually agreed Contract Documents.

2.3 If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by Supplier or on behalf of Google, including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms provided by Supplier or Google shall not take priority over this Contract Document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 Modification of Contract Terms and Contract Documents

3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.

3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 Definitions

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

- 4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.
- 4.2 **Addendum** means a mutually executed, written modification to a Contract Document.
- 4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.
- 4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.
- 4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.
- 4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.
- 4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.
- 4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.
- 4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.
- 4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.

- 4.11 Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.
- 4.12 Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.
- 4.13 Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 4.14 OAC** means the Oklahoma Administrative Code.
- 4.15 OMES** means the Office of Management and Enterprise Services.
- 4.16 Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.
- 4.17 State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.
- 4.18 Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State, and Google where applicable to fulfill obligations under the product and service terms, information security terms, and data protection terms, or as otherwise explicitly specified in this Contract.
- 4.19 Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.
- 4.20 Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.
- 4.21 Work Product** means, unless otherwise specified in a Task Order or Statement of Work, any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including

any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

- 5.1** Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.
- 5.2** Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.
- 5.3** The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer

requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

- 6.1** Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.
- 6.2** The State Chief Information Officer is a required signatory for any Acquisition made by State entities within the executive branch.
- 6.3** Supplier provides the Warranties as stated in the Google Cloud Master Agreement and applicable service schedules in Attachment E3 Section 8 and E5 Section 4 of this Contract .

Google further warrants that the Services provisioned will function in material conformance with the Documentation ("Performance Warranty"). If Google breaches this warranty, then Google will, in its discretion, correct the reported non-conformity for the impacted Service at no additional charge. If Google does not believe that this correction would be commercially reasonable, then upon Customer request (i) Google will refund to Customer any unused prepaid Fees that Customer paid to Google for use of the impacted Services, and (ii) if Customer has made financial commitments in an Order Form or addendum to the Agreement, then Google will agree to amend such commitments proportional to Customer's spend on the impacted Services in the year preceding the breach. This section states Customer's sole and exclusive remedy for Google's breach of the Performance Warranty.

The parties agree the acceptance terms below are default acceptance terms if acceptance is not addressed at the ordering level; however, acceptance can be negotiated at the ordering level and acceptance terms included in the ordering documents shall supersede the acceptance terms below.

Any professional services to be delivered pursuant to the Contract shall be subject to the acceptance terms described in subsections "a" through "d" below.

- a. Customer will have five (5) business days ("First Review Period") following receipt of a Deliverable from Google to determine whether

the Deliverable meets specific objective conditions described in a statement of work (“Acceptance Criteria”). If Customer provides notice of non-conformity in accordance with Section 6.2.b of the relevant statement of work, Customer will have up to two additional review periods of three (3) business days (“Second Review Period”) and three (3) business days (“Third Review Period”), as applicable, following receipt of a corrected Deliverable to confirm that the corrected Deliverable meets the applicable Acceptance Criteria.

- b. If Customer reasonably determines that a Deliverable does not conform to its Acceptance Criteria, then before the end of the applicable Review Period, Customer will provide written notice to Google describing in detail the nature of the non-conformity. If Customer does not provide notice of acceptance or non-conformity during the applicable Review Period, the Deliverable will be deemed accepted by the Customer.
- c. If Customer provides notice of non-conformity in accordance with Section 8 of the relevant statement of work for the First Review Period or Second Review Period, Google will, at no additional cost to the Customer, promptly make any changes reasonably required to correct the non-conformity described in the notice. Google will deliver the corrected Deliverable to the Customer.
- d. If Customer provides notice of non-conformity in accordance with Section 8 of the relevant statement of work Third Review Period, then unless the Parties agree otherwise in writing, Google will either, as applicable, (i) reduce any unpaid Fees by the amount due for the non-conforming Deliverable or (ii) return Fees in the amount paid for the non-conforming Deliverable, the portion of the Order Form applicable to the Deliverable will terminate, and Customer’s license to use the Deliverable will terminate.
- e. Any GCP services procured pursuant to this Contract are accepted when (1) both parties have executed a signed order form, (2) a valid Purchase Order is issued and (3) Google has made the GCP services available for use by the State as contracted for and intended by the parties.
- f. Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. Warranties for Services shall be described in the applicable Google Service Schedule.

- 6.4** Supplier shall deliver services on or before the required date specified in a Contract Document. Failure to deliver timely may result in the remedies as set forth in the applicable Contract Document. Google may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services. Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

- 7.1** Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted. This section shall not prohibit the payment to suppliers providing subscription services. For the purposes of this Section 7.1 “Supplier” shall mean Supplier’s public sector distributor, Carahsoft Technology Corporation, acting as Google’s agent for billing and invoicing services (the “Billing Agent”). The parties agree that the State shall accept invoices from, and remit payment to, the Billing Agent.

The following terms additionally apply:

- A.** An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.
- B.** Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.
- C.** Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.
- D.** The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.
- E.** If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.

- F. Supplier shall have no right of setoff.
- G. Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.
- H. The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

- 8.1** As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage, unless a lower subcontractor limit has been approved in writing by Customer. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better, or if self-insured, via Corporate Captive.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, where available, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and shall promptly provide proof to the State of any renewals, additions, or material changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

- A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;
- B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than \$5,000,000 per occurrence and in the aggregate;

- C. Automobile Liability Insurance with limits of liability of not less than \$5,000,000 combined single limit each accident;
- D. Employment Practices Liability coverage with limits not less than \$5,000,000 per occurrence;
- E. Professional Liability w/ Cyber Errors and Omissions insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits \$5,000,000 per occurrence; and
- F. Additional coverage required in writing, and as mutually agreed, in connection with a particular Acquisition.

- 8.2** Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.
- 8.3** Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from a failure by the Supplier to meet its tax, unemployment insurance, and/or Worker's Compensation obligations.
- 8.4** Customer represents, warrants, and covenants that (i) Customer's and any End Users' use of the Services, Customer Responsibility Materials, and Feedback will not violate this Agreement or applicable law; (ii) Customer Responsibility Materials or Feedback, the combination of Customer Responsibility Materials or Feedback with other applications, content, or processes, or the use, development, design, production, advertising, or marketing of Customer Responsibility Materials or Feedback, do not and will not infringe or misappropriate any third-party rights; and (iii) Customer's use of the Services will not cause harm to any End Users.

9 Compliance with Applicable Laws

- 9.1** As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:
- A.** Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.
 - B.** Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;
 - C.** Prospective participant requirements set at 2 C.F.R. part 376 in connection with Debarment, Suspension and other responsibility matters;
 - D.** 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;
 - E.** Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;
 - F.** Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein)
 - G.** Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify;
 - H.** Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

- I. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.
- 9.2 The Supplier's employees, agents and subcontractors shall adhere to the terms of this Contract including but not limited to the State of Oklahoma and Google LLC Agreed Information Security Requirements, Exhibit 1 to the March 2022 Cloud Master Agreement for the State of Oklahoma. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.
- 9.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.
- 9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory contract provisions when mutually agreed to by the parties and required in connection with the receipt of federal funds or other funding source.
- 9.5 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.
- 9.6 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.
- 9.7 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.
- 9.8 Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or

appointment of a receiver, liquidator or trustee through the disclosures in the Supplier's 10k.

- 9.9** Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.
- 9.10** If services provided by Supplier include delivery of an electronic communication, the extent to which a Supplier product is, prior to any customizations, capable of providing comparable access to individuals with disabilities consistent with the applicable provisions of the Architectural and Transportation Barriers Compliance Board standards set out in 36 CFR Part 1194 (known as 'Section 508'), effective as of June, 2001, or the Revised version in Appendix A (known as 'Revised Section 508') effective as of January, 2018 and the Web Content Accessibility Guidelines (WCAG) version 2.0 level AA, or the Web Content Accessibility Guidelines (WCAG) version 2.1 level AA is indicated by the dependencies, comments and exceptions (some of which may be significant, if any) noted on the applicable Accessibility Conformance Report (ACR) based on the Voluntary Product Accessibility Templates (VPAT) available at www.google.com/accessibility/customers-partners for each product, when they are used in accordance with Supplier's associated documents and other written information, and provided that any assistive technologies and any other products used with them properly interoperate with them. In the event that no ACR is available for a particular Supplier product, please contact the Supplier Accessibility Program Office at https://about.google/intl/ALL_us/belonging/disability-inclusion/product-accessibility/. In some cases, the outcome may be that a product is still being evaluated for accessibility, may be scheduled to meet accessibility standards in a future release, or may not be scheduled to meet accessibility standards at all. Supplier Support customers with disabilities may use the online portal: https://about.google/intl/ALL_us/belonging/disability-inclusion/product-accessibility/ to chat online with a specialist, request a phone call, send an email, or contact a specialist through the Be My Eyes App. The Disability Support team can help people who are deaf or hard-of-hearing through video chat with an American Sign Language (ASL) specialist. Supplier Support will respond to product accessibility issues according to the current Technical Support Policies. No other terms, conditions, statements or any other such representations regarding or related to accessibility shall apply to the Supplier products provided under the Contract. Supplier cannot make any commitments about future product directions, including plans to address accessibility or the availability of ACRs. Product direction remains at the sole discretion of Supplier.

10 Audits and Records Clause

- 10.1** As used in this clause and pursuant to 67 O.S. §203, “record” includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract. Each Party shall be responsible for their own costs of complying with this Section.
- 10.2** The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of three (3) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms.
- 10.3** Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

- 11.1** The provisions of Section 5 of the Cloud Master Agreement for the State of Oklahoma, Attachment E3 shall govern the Parties’ respective obligations with respect to the other Party’s Confidential Information.
- 11.2** Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director’s authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a

third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State and is contrary to the best interests of the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest contrary to the best interests of the State shall not occur without prior written approval of the State. Any violation of this Section 12 shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

- 13.1** Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.
- 13.2** Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, corporate restructuring, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and

all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

- 13.3** If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Subcontractors may be utilized in accordance with Section 12.6 of the Cloud Master Agreement between Google LLC and the State of Oklahoma, Attachment E3. If Google engages a new Google Subcontractor or changes the function of an existing Google Subcontractor (a “Subcontractor Change”), Google will inform Customer at least 30 days in advance, unless the Subcontractor Change is made to address an existing or imminent risk to the Services, in which case Google will provide Customer as much advance notice as is reasonably possible. If Customer determines that a Subcontractor Change would materially increase Customer’s risk or Google does not inform Customer of a Subcontractor Change as required in this Section 13.3, Customer may terminate the Order Form for the Services under 11.2 (Termination for Convenience) of Attachment E3.
- 13.4** All payments under the Contract shall be made directly to the Supplier, except as provided in subsection 13.1 above regarding the Supplier’s assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.
- 13.5** Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. Prior to the commencement of any services, background checks and criminal history investigations of the Supplier’s employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier’s access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. If the State has identified and requests that a heightened background check, or fingerprinting, is required, then Google will ensure that its subcontractor complies with such a requirement before any work is performed. The State must notify Google in writing of any heightened background check before the start of work. Any

heightened background check may extend the performance periods described in the relevant statement of work. Any schedule extension caused by a heightened background check will not reduce the pricing described in the relevant statement of work. Should Customer become aware of additional background check or fingerprinting requirements during the performance period of a statement of work, Customer and Google will engage in discussions and will agree on a plan to ensure both parties comply with applicable laws and regulations, which may include, if necessary, Customer background checks.

The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property, copyright or other property right, the Parties' rights shall be as stated in Section 9, Indemnification, of the Google Cloud Master Agreement for the State of Oklahoma, Attachment E3.

16 Indemnification

16.1 Acts or Omissions

- A.** Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or

claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.

- B.** To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Indemnification for Intellectual Property Infringement shall be as Stated in Section 9.1 of the Google Cloud Master Agreement for the State of Oklahoma, Attachment E3

16.3 Notice and Cooperation

Subject to Section 9.4 of the Google Cloud Master Agreement for the State of Oklahoma, Attachment E3, in connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened

lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

The applicable Limitation of Liability shall be that contained in Section 10 of the Google Cloud Master Agreement for the State of Oklahoma, Attachment E3.

17 Termination for Funding Insufficiency

17.1 Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

17.2 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.

- 17.3** The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

- 18.1** Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.
- 18.2** The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.
- 18.3** Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

18.4 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Reserved.

19.1 The State may terminate the Contract, including (unless specified otherwise) any orders of the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Upon such termination, the Supplier shall provide a pro rata refund of any prepaid fees for services or goods that were not delivered as of the effective date of termination unless the State has elected to terminate an enterprise agreement or an agreement where a discounted price was applied conditioned upon the State's commitment to a specific term, level of use, or allocation. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.

20 Suspension of Supplier

20.1 The parties agree that the suspension terms below are not applicable to any cloud systems procured pursuant to this Contract.

20.2 Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.

20.3 Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the

incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

- 20.4** Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract. A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

- 23.1** Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has

prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

- 23.2** Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.
- 23.3** Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

Under the Contract, notices to Customer must be sent to the Notification Email 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.

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

On termination or expiration of the Contract or an Order Form, Google will continue to provide the Services in accordance with the terms of the Contract for up to 12 months (the "Transition Term") provided that: (i) Customer requests a Transition Term in writing before the relevant termination or expiration date; and (ii) Customer is only entitled to one Transition Term.

During the Transition Term, Customer may make a written request for advisory and implementation services from Google to assist in migrating workloads and applications or otherwise transitioning Customer's use of the Services ("Transition Assistance"). Google will provide Transition Assistance to Customer subject to the Implementation Services Schedule or such other

agreement between Google and Customer under which Google agrees to provide advisory and implementation services to Customer. These terms will describe the scope of the Transition Assistance and any applicable fees.

26.5 Publicity

Any marketing and publicity shall be subject to Section 6 of the Google Cloud Master Agreement for the State of Oklahoma, Attachment E3

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq.* Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

- A.** No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.
- B.** The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.
- C.** The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.
- D.** The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.

- E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain

payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms (“Information Technology Terms”), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services (“OMES-IS”) is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

- 1.1 **COTS** means software that is commercial off the shelf.
- 1.2 **Customer Data** means data provided to Google by Customer or End Users through the Services under the Account, and data that Customer or End Users derive from that data through their use of the Services.
- 1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.
- 1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.
- 1.5 **Intellectual Property Rights** means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.
- 1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

- 1.8 Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.
- 1.9 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. Google will notify Customer promptly and without undue delay, in no case more than 24 hours after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.
- 1.10 State CIO** means the State Chief Information Officer or authorized designee.
- 1.11 Work Product** means, unless otherwise specified in a Task Order or Statement of Work, any and all deliverables produced by Supplier for Customer under a statement of work or similar Contract Document issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2 Termination of Maintenance and Support Services

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

- 2.1** Google discontinues the product for which the services are provided; or
- 2.2** If Customer chooses to renew maintenance or support after maintenance has lapsed,

Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Subject to any financial commitments on an Order Form, any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards (“Standards”) set forth at <https://oklahoma.gov/omes/services/information-services/is/policies-and-standards/accessibility-standards.html>. The Parties agree that Google’s accessibility conformance reports, contained <https://cloud.google.com/security/compliance/vpat>, are available for review. The Parties further agree that Google does not control how third parties and integrators use its cloud products to build their own websites, and so makes no representations regarding their 508 Compliance. Additionally, Google clarifies that it represents its compliance as stated in those reports and takes exception to any certification beyond those contained therein.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

- 4.1** Disk drives and memory cards will not be provided by Supplier in conjunction with Services delivered by Supplier under the Contract. Any disk drives and memory cards purchased by OMES-IS for use in leased or purchased products under the Contract remain the property of the Customer.
- 4.2** Hardware and physical media will not be provided by Supplier in conjunction with Services delivered by Supplier under the Contract.

5 Offshore Services

- 5.1** Pursuant to Exhibit 1 of the Google Cloud Master Agreement for the State of Oklahoma Attachment E2 - State of Oklahoma and Google LLC Agreed Information Security Requirements, Oklahoma may configure the requirements to ensure no offshore services are provided. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow the sun model which may be used by Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 Compliance with Technology Policies

- 6.1** The FedRAMP Board has issued FedRAMP Moderate and FedRAMP High Authority to Operate (ATO) to Google Cloud infrastructure and to specific Google Cloud Services Offerings (CSOs). Google Cloud routinely submits additional services for FedRAMP Moderate and High approvals to the Board. Google Cloud can provide the following additional FedRAMP compliance documentation to customers under non-disclosure agreement (NDA): FedRAMP Customer Responsibility Matrix (CRM), Google Cloud’s

System Security Plan (SSP), Penetration test reports and other documents. To use Google Cloud services in alignment with FedRAMP Moderate or High levels, hosting must use Assured Workloads and Assured Support (High only). A list of services in-scope can be found at the following hyperlink: <https://cloud.google.com/security/compliance/fedramp>

- 6.2** Google will maintain the Compliance Certifications and SOC Reports as described in the Data Processing and Security Terms.

7 Emerging Technologies

- 7.1** The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

- 8.1** In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State and if applicable the prices during any such extension will be subject to mutual agreement of the parties.

9 Source Code Escrow

- 9.1** The Parties do not anticipate that Supplier will develop customized computer software or any modifications exclusively for a State agency. If a Task Order is issued under this contract that requires such work, then the Parties will negotiate appropriate terms in compliance with 62 O.S. § 34.31.

10 Commercial Off The Shelf Software

- 10.1** If Supplier or Google specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

- 11.1** With respect to any Deliverables developed by the Supplier under the terms of the Contract that are not customized, modified, or developed exclusively for the State, the parties agree that Section 3.2 of the Implementation Service Schedule to the Google Cloud Master Agreement with the State of Oklahoma shall govern ownership and licensing, Attachment E5.

12 Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

- 12.1** With respect to any orders for Google Cloud Platform products, the provisions of Section 4 of the Google Cloud Master Agreement with the State of Oklahoma, Attachment E3 shall

apply.

- 12.2** With respect to any orders for products from the Implementation Services Schedule, the provisions of Section 4 of the Google Cloud Master Agreement and Section 3 of the Implementation Service Schedule to the Google Cloud Master Agreement with the State of Oklahoma, Attachment E5 shall apply.

13 Hosting Services

- 13.1** If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.
- 13.2** If a Data Breach or Data Incident occurs , Google shall be responsible for the obligations set forth in Appendix 1, excluding damages that are the sole fault of the Customer (and any contributory fault by Customer as agreed by the parties or determined by a court of competent jurisdiction shall result in a reduction of damages to reflect only the actual fault of Supplier) related to breach reporting requirements and associated costs.

14 Change Management

- 14.1** Section 4 of the Google Cloud Platform Services Schedule to the Google Cloud Master Agreement with the State of Oklahoma, Attachment E4 shall apply to any updates to products or services.

15 Service Level Deficiency

- 15.1** In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, as defined in the applicable Service Schedule attached to the Contract, service credits shall be provided by Supplier in accordance with the terms of the applicable Service Schedule and the SLAs described therein.

16 Notices

- 16.1** Under the Contract, notices to Customer must be sent to the Notification Email 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.

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to as described in the Data Processing and Security Terms.
2. Reserved.
3. Supplier and Google will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier as described in the Data Processing and Security Terms. Google will notify Customer promptly and without undue delay, in no case more than 24 hours after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

1. Google shall implement and maintain the Security Measures described in the Data Processing and Security Terms.
2. Google Cloud Platform encrypts customer data stored on its servers by default using one or more encryption keys, as further described in the Data Processing and Security Terms. Data moving between GCP services or between the client and Google Cloud Platform is typically protected using HTTPS or other industry-standard protocols. Google will make available to the State tools, measures, and training to ensure all Personal Data and Non-public Data can be encrypted at rest and in transit with controlled access. Further Google agrees to maintain and upgrade said tools to ensure ongoing effectiveness as described in the Data Processing and Security Terms.
3. Google will implement tools, measures, and training designed to prevent the introduction of any viruses, worms, spyware, or any other similar devices or mechanisms ("Viruses")

into the Services or Software that it provides. Further Google agrees to maintain and upgrade said tools to ensure ongoing effectiveness. For the avoidance of doubt, Customer is responsible for preventing the introduction of Viruses into its environment in connection with its use of the Services or the Software.

4. Supplier shall allow the Customer to audit conformance to the Contract terms in accordance with the Data Processing and Security Terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.
5. Google shall perform an independent audit of its data centers as described in the Data Processing and Security Terms and make the Security Documentation available for review by Customer, at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or equivalent, as set forth in the Data Processing and Security Terms, sets the minimum level of a third- party audit.
6. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards during the term of the contract, including renewals, constitutes a material breach. Supplier shall provide updated data security information as described in ATTACHMENT E2 State of Oklahoma and Google LLC Agreed Information Security Requirements Section 1 "General Information Security Requirements".

D. Data Incident or Data Breach Notification: Google shall inform Customer of any Data Incident or Data Breach as described in the Data Processing and Security Terms. Google will notify Customer promptly and without undue delay, in no case more than 24 hours after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

E. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Google shall as described in the Data Processing and Security Terms (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

2. Notwithstanding Section 11.1(a) and Section 10.3 (Exclusions) of Attachment E3, Customer may recover Remediation-Related Costs that directly result from a Security Obligation Breach, subject to the limitations in Section 10.1(b) (Limitation on Amount of Liability).

F. Notices

1. Under the Contract, notices to Customer must be sent to the Notification Email 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.

G. Supplier Representations and Warranties

Supplier states the following with respect to Indemnification, Confidentiality, Existing Contracts, and Viruses:

1. Subject to Customer Indemnification Obligations and Supplier's Remedies for suspected infringement being provided in Attachment E3, as of the Contract Effective Date the product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.
2. Google will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination as described in the Data Processing and Security Terms, and with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.
3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.
4. Google shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or through the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. Indemnity

1. Indemnification terms for this Contract are reflected in Attachment E3 Section 9.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Google shall not take any action to intentionally

disclose, alter or erase any Customer Data.

2. In the event of a termination or expiration of the Contract, Data Deletion policies are described in the Data Processing and Security Terms.
3. The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

Appendix 2 to State of Oklahoma Information Technology Terms

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation (“FBI”), Criminal Justice Information Services (CJIS) Division’s CJIS Security Policy (“CJIS Security Policy” or “Security Policy” herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer (“CSO”) and the FBI CJIS Division’s Audit Staff.

The Parties agree that to the terms of Attachment C, Criminal Justice Information Services Information Addendum, to the State of Oklahoma and Google LLC Agreed Information Security Requirements, Attachment E2.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

This FBI Security Policy is located and may be downloaded at: <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist Compliance checklist –

Policy Area 1 Information Exchange Agreements Policy

Area 2 Security Awareness Training Policy Area

3 Incident Response

Policy Area 4 Auditing and Accountability

Policy Area 5 Access Control

Policy Area 6 Identification and Authentication

Policy Area 7 Configuration Management

Policy Area 8 Media Protection

Policy Area 9 Physical Protection

Policy Area 10 Systems and Communications
Protection and Information
Integrity

Policy Area 11Formal Audits Policy

Area 12Personnel Security

ATTACHMENT E1

ADDITIONAL TERMS

SecOps Services Schedule

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

1. Using the Services.

1.1 *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 and associated passwords, including any keys for Google APIs, if any, and (b) any use of the Account.

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

1.3 *Additional Use Restrictions.* Customer will not use the Services to provide a hosting, outsourced, or managed services solution to unaffiliated third parties.

2. Data Processing and Security. Google will only access, use, and otherwise process Customer Data in accordance with this Contract and 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.

3. Additional Payment Terms.

3.1 *Usage and Invoicing.* Customer will pay all Fees for the Services and Technical Support Services. 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.

3.2 *Suspension for Overdue Payment.* Google may Suspend the Services under General Terms Section 3.4(a) (Overdue Payments) only if Customer's payment is overdue for more than 14 days after the Payment Due Date. Google will notify Customer at least 7 days before Suspension.

4. Updates to Services and Terms.

4.1 *Changes to Services.*

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

(b) *Discontinuance.* Notwithstanding Section 4.1(a) (Limitations on Changes), Google may discontinue a Service (or associated material functionality) provided that Google will notify Customer at least 12 months before discontinuing such Service (or associated material

functionality), unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

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

(d) **Backwards Incompatible Changes.** Notwithstanding Section 4.1(a) (Limitations on Changes), Google may significantly modify a Customer-facing Google API in a backwards-incompatible manner, provided that Google will notify Customer at least 12 months before doing so.

4.2 Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Cloud Data Processing Addendum, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material changes to the URL Terms. Material changes to the URL Terms will be effective 30 days after Customer receives notice of such changes.

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

5. Temporary Suspension.

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

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

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

7. 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.

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

9. Survival. The following Sections of this Services Schedule will survive expiration or termination of this Services Schedule: Section 12 (Additional Definitions).

11. Termination of Previous Agreements. If Google, including its Affiliates, and Customer have previously entered into an agreement for the Services, then the parties agree that this Agreement will govern the provision and use of the Services going forward.

12. Additional Definitions.

"Account" means the account that Google assigns to Customer to access the Services.

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

"Cloud Data Processing Addendum" 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>. For Mandiant Consulting Services and Mandiant Managed Services only, the Cloud Data Processing Addendum is at <https://cloud.google.com/terms/secops/data-processing-addendum>.

"Covered Affiliate" means a Customer Affiliate that uses the Services under the Agreement.

"Customer Data" means data provided to Google by Customer or End Users through the Services under the Account, and data that Customer or End Users derive from that data through their use of the Services.

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

"Data Processing Terms" means the Cloud Data Processing Addendum.

"End User" or "Customer End User" means an individual that Customer permits to use the Services. For clarity, End Users may include employees of Customer.

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

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

"Notification Email Address" means the email address(es) designated by Customer in the applicable Order Form, or if none exists, the email address for Customer's primary contact.

"Order Form" means (a) an order form, statement of work, or other ordering document issued by Google under the 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.

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

"Prices" means the prices for the Services, Software, and Technical Support Services as described in an Order Form or amendment to this Services Schedule.

"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 the 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.

"SecOps Service Specific Terms" means the then-current terms specific to one or more Services or Software, at <https://cloud.google.com/terms/secops/service-terms>.

"Services" means the then-current services described at <https://cloud.google.com/terms/secops/services>, excluding any Third-Party Offerings.

"SLA" means the then-current service level agreements at <https://cloud.google.com/terms/secops/sla>.

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

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

"Technical Support Services Guidelines" or "TSS Guidelines" means the then-current Google support service guidelines, at <https://cloud.google.com/terms/secops/tssg>.

"Third-Party Offerings" means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software, and (b) third-party operating systems.

"URL Terms" means the AUP, Cloud Data Processing Addendum, SecOps Service Specific Terms, SLAs, and Technical Support Services Guidelines. The URL Terms for SecOps Services are all available at <https://g.co/cloud/secops-directory-terms>.

13. Regional Terms. Customer agrees to the following modifications to the Agreement if Customer's billing address is in the applicable region as described below:

Asia Pacific - India

For purposes of this Services Schedule, the following will apply:

(a) Except as described in (b) below, 'Google' will mean 'Google Asia Pacific Pte Ltd' or 'GAP'. The entire obligation to provide the Services will be met by GAP, and as such, Google Cloud India will not have any obligation to provide the Services;

(b) For any right or obligation related to invoicing, Prices, Taxes, or payments, 'Google' will mean 'Google Cloud India'.

Brazil

For the purposes of this Services Schedule, 'Google' means 'Google Cloud Brasil Computação e Serviços de Dados Ltda', except if provided otherwise in the respective Order Form.



ATTACHMENT E2

State of Oklahoma and Google LLC Agreed Information Security Requirements

Customer Configuration Requirements

- a. Using Google Assured Workloads, Customer must classify Customer data to support the requirements of CJI, FTI, SSA, and Child Support FPLS data. Assured Workloads configuration instructions are available at: <https://cloud.google.com/assured-workloads/docs/how-to-get-started>.
- b. In addition to using Assured Workloads, Customer must purchase Premium Support with Assured Support or Enhanced Support with Assured Support to ensure compliance with requirements concerning CJI, FTI, SSA, and Child Support FPLS data.

1. General Information Security Requirements

- a. Google data protection responsibilities are described in its Data Processing and Security Terms (DPST), which is available at: <https://cloud.google.com/terms/data-processing-terms>. As described in the DPST, Google will notify Customer promptly and without undue delay, in no case more than 24 hours after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.
- b. 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.

2. HIPAA Requirements

- a. Google shall agree to use and disclose Protected Health Information in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).
- b. Contractor's Business Associate Agreement is attached as Attachment A

3. 42 C.F.R. Part 2 Related Provisions

- a. Confidentiality of Information. Google's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms

of this Agreement. Google accepts the responsibilities for providing adequate supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Google:

- b. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A§ 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;
- c. Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of any kind;
- d. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;
- e. Agrees to use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).
- f. As provided for in the Google Data Processing and Security Terms, agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement.
- g. Agrees to enable access to the protected information in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;
- h. intentionally omitted;
- i. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the

State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

- j. Agrees to enable the State of Oklahoma agency, or an authorized individual, to receive information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.
- k. **Data Security.** Google agrees to maintain the data in a secure manner compatible with the content and use. Google will control access to the data in compliance with the terms of this Agreement. Only Google's personnel whose duties require the use of such information, will have regular access to the data. Google's employees will be allowed access to the data only for the purpose set forth in this Agreement.
- l. intentionally omitted.
- m. **Use of Information.** Google agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.
- n. **Redislosure of Data.** Google agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redislosure is permitted under applicable law.
- o. The requirements contained in this section only apply to the extent applicable to Google.
- p. The State of Oklahoma is responsible for obtaining any consents required by law to disclose data to Google. Google will cooperate and provide assistance to the State of Oklahoma.

4. Federal Tax Information Requirements

- a. Google's IRS 1075 addendum is attached as Attachment B.

5. SSA Requirements

- a. **PERFORMANCE:** In performance of this contract, the Google agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:
 - i. All work will be done under the supervision of Google or Google's employees.
 - ii. Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Google is prohibited.

- iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
- iv. No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.
- v. Google shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.
- vi. Google or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. The State of Oklahoma will provide proof of this authorization to the Contractor before the State of Oklahoma stores any data on Customer's cloud platform.
- vii. Google shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Google is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful access and/or disclosure.
- viii. Google shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Google shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.
- ix. The applicable State of Oklahoma agency shall provide the Google a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Google is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from Google a current list of the employees with access to SSA data and provide such list to the SSA.
- x. Where Google processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of Google within the Agreement.
- xi. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

- xii. SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.
 - xiii. If Google must send a computer, hard drive, or other computing or storage device offsite for repair, the Google must have a non-disclosure clause in their contract with the vendor. If Google used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect Google's vendor contract. Google must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects Google to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.
 - xiv. In the event of a suspected or verified data breach involving SSA provided information, Google shall notify the Client as described in Google's Data Processing and Security Terms.
 - xv. The Client shall have the right to void the contract if Google fails to provide the safeguards described above.
- b. **CRIMINAL/CIVIL SANCTIONS:** The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act.

The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder.

An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act.

Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.

i. **Civil Remedies.**

- (1) In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of -
 - (a) actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of \$1,000; and

(b) the costs of the action together with reasonable attorney fees as determined by the court.

- (2) An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ii. Criminal Penalties

- (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(1).
- (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(2).
- (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000. See 5 U.S.C. § 552a(i)(3).

6. Child Support FPLS Requirements

- a. Google and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Google and applicable State of Oklahoma agency also agree

to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

- i. This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Google, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.
- ii. This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

7. FERPA Requirements

- a. In performance of this Agreement, Google agrees to comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

8. CJIS Requirements

- a. Google's Criminal Justice Information Services Information Addendum is attached as Attachment C.

**Attachment A to
State of Oklahoma and Google LLC Agreed Information Security Requirements**

The HIPAA Business Associate Addendum is hereby amended as set forth below and supersedes all prior documents submitted by Google LLC or discussed by the parties. The parties agree to use this HIPAA Business Associate Addendum or a document substantially similar in the form of this HIPAA Business Associate Addendum.

[Remainder of page intentionally blank]

ATTACHMENT A

HIPAA BUSINESS ASSOCIATE ADDENDUM

This HIPAA Business Associate Addendum ("BAA") is entered into between Google LLC ("Google") and [the Customer], with offices at [Customer's Physical Address] ("Customer"), and supplements, amends and is incorporated into the Services Agreement, defined below.

Capitalized terms used but not defined in this Addendum have the meaning given to them in the Services Agreement. This BAA will be effective as of the last signature date below (the "BAA Effective Date").

Customer must have an existing Services Agreement in place for this BAA to be valid and effective. Together with the Services Agreement, this BAA will govern each party's respective obligations regarding Protected Health Information (defined below). Customer agrees that the terms of the Services Agreement applies to the provision and use of the Covered Services.

This BAA (a) only applies to Covered Services provided under the Services Agreement, (b) is valid and effective so long as there is an active Order Form for such Covered Services, and (c) together with the Services Agreement, governs each party's respective obligations regarding Protected Health Information. Changes to this BAA must be mutually-agreed upon by both parties.

1. Definitions.

"Business Associate" has the definition given to it under HIPAA.

"Breach" has the definition given to it under HIPAA.

"Covered Entity" has the definition given to it under HIPAA.

"Covered Services" means the Google products and/or services specifically listed in the URLs on Attachment 1, as may be updated from time to time by Google with notice to Customer.

Google may only remove a Covered Service from those URLs with at least 12 months prior notice.

"Designated Record Set" has the definition give to it under HIPAA.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended.

"HIPAA Implementation Guide" means the informational guide that Google makes available at the URL in Attachment 2, or a successor URL, describing how the Covered Services may be configured by Customer in connection with Customer's HIPAA compliance efforts.

"HITECH Act" means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.

"Protected Health Information" or "PHI" has the definition given to it under HIPAA and for purposes of this BAA is limited to PHI within Customer Data to which Google has access through the Covered Services in connection with Customer's permitted use of Covered Services.

"Required by Law" has the definition given to it under HIPAA.

"Security Incident" has the definition given to it under HIPAA.

"Services Agreement" means the Google Cloud Master Terms-Public Sector and the Google Cloud Master Agreement Services Schedule that Customer accepted as part of the Customer's agreement with a Google authorized distributor or reseller for the provision of the Covered Services.

2. **Applicability.** This BAA applies to the extent Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via a Covered Service and to the extent Google, as a result, is deemed under HIPAA to be acting as a Business Associate or Subcontractor of Customer. Customer acknowledges that this BAA does not apply to (a) any other Google product, service, or feature that is not a Covered Service; or (b) any PHI that Customer creates, receives, maintains, or transmits outside of the Covered Services (including Customer's use of its offline or on-premise storage tools or third-party applications).

3. **Permitted Use and Disclosure of PHI.**

- (a) Except as otherwise stated in this BAA, Google may use and disclose PHI only (i) as permitted or required by the Services Agreement or this BAA or (ii) as required by law.
- (b) Google may use and disclose PHI for its proper management and administration and to carry out its legal responsibilities, provided that any disclosure of PHI for such purposes may only occur if (i) required by law; or (ii) Google obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Google will be notified of any Breach or Security Incident.

4. **Customer Obligations.**

- (a) Customer will not request that Google or the Covered Services use or disclose PHI in any manner that would not be permissible under HIPAA if done by Customer (if Customer is a Covered Entity) or by the Covered Entity to which Customer is a

Business Associate (unless expressly permitted under HIPAA for a Business Associate).

- (b) For End Users that use the Covered Services in connection with PHI, Customer will use controls available within the Services, including those detailed in the HIPAA Implementation Guide, to ensure its use of PHI is limited to the Covered Services. Customer acknowledges and agrees that the HIPAA Implementation Guide is provided by Google solely as an informational guide with respect to Customer's configuration options, and that Customer is solely responsible for ensuring that its and its End Users' use of the Covered Services complies with HIPAA and HITECH.

5. **Appropriate Safeguards.** Google and Customer will each use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Covered Services.

6. **Reporting and Related Obligations.**

- (a) Google will promptly notify Customer of (i) any Security Incident of which Google becomes aware, subject to Sections 6(b) and 6(c); and (ii) any Breach that Google discovers, provided that any notice for Breach will be made promptly and without unreasonable delay, and in no case more than 24 hours after discovery. Notifications made under this section will describe, to the extent possible, details of a Breach, including steps taken to mitigate the potential risks and steps Google recommends Customer take to address the Breach.
- (b) Google will send any applicable notifications to the notification email address provided by Customer in the 1AM & Admin/Essential Contacts field found in the Google Cloud Platform Admin Console, provided that Customer first checks the box entitled "Security." Customer is solely responsible for keeping its email address up to date and for ensuring that the "Security" box remains checked.
- (c) Notwithstanding Section 6(a), this Section 6(c) will be deemed as notice to Customer that Google periodically receives unsuccessful attempts for unauthorized access, use, disclosure, modification, or destruction of information, or interference with the general operation of Google's systems and the Covered Services. Customer acknowledges and agrees that even if such events constitute a Security Incident, Google will not be required to provide any notice under this BAA regarding such unsuccessful attempts other than this Section 6(c).

7. **Subcontractors.** Google will take appropriate measures to ensure that any Subcontractors used by Google to perform its obligations under the Services Agreement that require access to PHI on behalf of Google are bound by written obligations that provide the same material level of protection for PHI as this BAA. To the extent Google uses Subcontractors in its performance of obligations hereunder, Google will remain responsible for their performance as if performed by Google.

8. **Access and Amendment.** Customer acknowledges and agrees that Customer is solely responsible for the form and content of PHI maintained by Customer within the Covered Services, including whether Customer maintains such PHI in a Designated Record Set within the Covered Services. Google will provide Customer with access to Customer's PHI via the Covered Services so that Customer may fulfill its obligations under HIPAA with respect to Individuals' rights of access and amendment, but will have no other obligations to Customer or any Individual with respect to the rights afforded to Individuals by HIPAA with respect to Designated Record Sets, including rights of access or amendment of PHI. Customer is responsible for managing its use of the Covered Services to appropriately respond to such individual requests.
9. **Accounting of Disclosures.** Google will document disclosures of PHI by Google and provide an accounting of such disclosures to Customer as and to the extent required of a Business Associate under HIPAA and in accordance with the requirements applicable to a Business Associate under HIPAA. Google will bear the costs associated with notifications to individuals, regulators or others required by federal or state law, but, to the extent permitted by law, will be subject to Section 10 (Liability) of the Google Cloud Master Agreement General Terms.
10. **Access to Records.** To the extent required by law, and subject to applicable attorney client privileges, Google will make its internal practices, books, and records concerning the use and disclosure of PHI received from Customer, or created or received by Google on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this BAA.
11. **Expiration and Termination.**
 - (a) This BAA will terminate on the earlier of (i) a permitted termination in accordance with Section 11(b), or (ii) the expiration or termination of the Services Agreement under which Customer has access to a Covered Service.
 - (b) If either party materially breaches this BAA, the non-breaching party may terminate this BAA on 10 days' written notice to the breaching party unless the breach is cured within the 10-day period. If a cure under this Section 11(b) is not reasonably possible, the non-breaching party may immediately terminate this BAA, or if neither termination nor cure is reasonably possible under this Section 11(b), the non-breaching party may report the violation to the Secretary, subject to all applicable legal privileges.
 - (c) If this BAA is terminated earlier than the Services Agreement, Customer may continue to use the Services in accordance with the Services Agreement, but must delete any PHI it maintains in the Covered Services and cease to further create, receive, maintain, or transmit such PHI to Google.

12. **Return/Destruction of Information.** On termination of the Services Agreement, Google will return or destroy all PHI received from Customer, or created or received by Google on behalf of Customer; provided, however, that if such return or destruction is not feasible, Google will extend the protections of this BM to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

13. **Miscellaneous.**

- (a) Survival. Sections 12 (Return/Destruction of Information) and 13 (Miscellaneous) will survive termination or expiration of this BM.
- (b) Counterparts. The parties may execute this BM in counterparts, including facsimile, PDF, or other electronic copies, which taken together will constitute one instrument.
- (c) Effects of Addendum. The Services Agreement remains in full force and effect except as modified by this BM. To the extent the Services Agreement and this BM conflict, this BM governs.

Signed by the parties' authorized representatives on the dates below.

Google

By:

Print

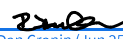
Title:

Date:


Philipp Schindler
Authorized Signatory

2025.06.24
09:32:01
-07'00'

Customer

By: 
Dan Cronin (Jun 25, 2025 09:45 CDT)

Print Name: Dan Cronin

Title: State Chief Information Officer

Date: Jun 25, 2025

Attachment 1

List of Covered Services

- Any Google Workspace product or service specifically identified at:
http://cloud.google.com/terms/identity/hipaa_functionality.html as being covered by the Google BAA (collectively "Google Workspace Covered Services").
- Any Google Cloud Platform product or service specifically identified at
<https://cloud.google.com/security/compliance/hipaa/> as being covered by the Google BAA (collectively "GCP Covered Services").

Attachment 2
HIPAA Implementation Guide

For Google Workspace Covered Services:

- The HIPAA Implementation Guide is available for review at the following URL:
https://static.googleusercontent.com/media/gsuite.google.com/en//terms/2015/1/hipaa_implementation_guide.pdf

For GCP Covered Services:

- The HIPAA Implementation Guide is available for review at the following URL:
<https://cloud.google.com/security/compliance/hipaa/>

ATTACHMENT B

INTERNAL REVENUE SERVICE PUBLICATION 1075 ADDENDUM

This Internal Revenue Service Publication 1075 Addendum ("Addendum") is for the use of Google Cloud Platform by state and local government agencies of the State of Oklahoma and is entered into by Google LLC, with offices at 1600 Amphitheatre Parkway, Mountain View, CA 94043 ("Google") the State of Oklahoma by and through the Office of Management and Enterprise Services ("Customer"). Customer must have an existing Services Agreement in place for this Addendum to be valid and effective.

Together with the Services Agreement, this Addendum will govern each party's respective obligations regarding the protection of Federal Tax Information of any Customer as that term is defined in Internal Revenue Service Publication 1075, Version 11-2021. Customer agrees that the terms of the Services Agreement apply to the provision and use of the Google Cloud Platform Services. It is mutually understood any Federal Tax Information of the State of Oklahoma contained within Google's covered services is covered by the requirements of Internal Revenue Service Publication 1075, subject to Customer's compliance with Subsection 1 of this Addendum.

1. Disclosure.

As of the Effective Date, which is the date of the last signature below, Google, through its Assured Workloads for Government product, allows the Customer to comply with the requirements of 26 C.F.R. 301.6103(n)-1 and IRS Publication 1075 (November 2021) (collectively the "IRS Rules"). In addition to using Assured Workloads for Government, Customer must purchase Google Premium Support with Assured Support or Enhanced Support with Assured Support to ensure compliance with the IRS Rules.

The Customer is responsible for using Google Cloud Platform in accordance with the IRS Rules noted above as well as all applicable conditions and restrictions contained in IRS regulations, IRS published rules, or IRS procedures.

2. Federal Tax Information Requirements.

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

- (1) All work will be performed under the supervision of the contractor.
- (2) The contractor and contractor's officers or employees to be authorized access to FTI must

meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officer or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

- (3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- (4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- (5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- (7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- (8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- (9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- (10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.
- (11) In addition to the subcontractor's obligations and duties under an approved subcontract,

the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

- (12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
- (13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

11. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
- (2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
- (3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

- (4) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 ([see Exhibit 4, *Sanctions for Unauthorized Disclosure*](#), and [Exhibit 5, *Civil Damages for Unauthorized Disclosure*](#)). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

111. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

ATTACHMENT C

CRIMINAL JUSTICE INFORMATION SERVICES INFORMATION ADDENDUM

This CJIS Information Addendum ("Addendum") is for the use of Google Cloud Platform by state and local government agencies of the State of Oklahoma and is entered into by Google LLC, with offices at 1600 Amphitheatre Parkway, Mountain View, CA 94043 ("Google") and State of Oklahoma by and through the Office of Management and Enterprise Services ("Customer"). Google and Customer must have an existing Services Agreement, or other agreement that allows the State of Oklahoma to purchase Google services, in place for this Addendum to be valid and effective.

Together with the Services Agreement, this Addendum will govern each party's respective obligations regarding the protection of Criminal Justice Information as that term is defined in the Criminal Justice Information Services Security Policy, Version 5.9, June 1, 2020. Customer agrees that the terms of the Services Agreement apply to the provision and use of the Covered Services.

Customer agrees that the terms of the Services Agreement apply to the provision and use of the Covered Services. This Addendum only applies when Customer purchases Assured Workloads, and purchases Premium Support and Assured Support or Enhanced Support and Assured Support. Other than Assured Workloads, none of the other Google Cloud Platform services are covered by this Addendum.

Agreement General Terms

1. Definitions.

"Agency Affiliate" means any governmental agency, department, office, instrumentality, division, unit or other entity established under the laws of Customer and operating within Customer's jurisdiction, that is subject to the CJIS Security Policy and is a party to an end user agreement with Customer for access to the Customer Information Enforcement System.

"Authorized Google Personnel" means Google Personnel that have successfully met the screening criteria in accordance with Section 5.4.a.

"Authorized Reseller" means an organization that has been authorized by Google or a Google Affiliate to resell and/or distribute Covered Services.

"CJIS Security Policy" means the FBI CJIS Security Policy version 5.9, dated June 1, 2020 (as updated or amended).

"Confidential Information" means information that one party discloses to the other party under the Agreement or other agreement that allows Customer to purchase Google services, and that

is marked as confidential, privileged, or trade secret, or would normally be considered confidential or competitively sensitive information under the circumstances, or is confidential by law. Confidential Information does not include information that is independently developed by the recipient, is shared with the recipient by a third party without confidentiality obligations, or is or becomes public through no fault of the recipient.

"Covered Affiliates" means an Agency Affiliate that purchases Covered Services under GCP Terms.

"Covered Services" means those Services found here:
<https://cloud.google.com/security/compliance/cjishe>

"Criminal Justice Information" ("CJI") is defined in the Criminal Justice Information Services Security Policy, Version 5.9, June 1, 2020.

"Criminal Justice Information Services Division" ("FBI CJIS" or "CJIS") means the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

"Effective Date" means the date of the last party's signature of the Addendum.

"GCP Terms" means: (a) Google's standard commercial agreement that governs the use of Google Cloud Platform, including applicable Data Processing and Security Terms ("DPST"); or
(b) an Authorized Reseller's commercial agreement that governs the use of Google Cloud Platform, as applicable.

"General Terms" means Sections 1 - 8 of this Agreement.

"Google Personnel" means employees or contractors employed or engaged by Google or its Affiliates.

2. CJIS Security Addendum.

The Covered Services are multi-tenant cloud services provided by Google Cloud data centers for use by government, commercial and consumer customers, and offered as a "community cloud" as defined in the National Institute of Standards and Technology (NIST) Special Publications 800-145. Subject to the Google Cloud Master Agreement Google Cloud Platform Services Schedule, the Covered Services will be delivered in accordance with the CJIS Security Addendum in Schedule 1 to this Agreement (Security Addendum).

3. Agency Role on behalf of Covered Affiliates.

3.1 Google and Customer are entering into this Addendum to facilitate the use of Covered Services by Customer and Agency Affiliates. The Oklahoma Department of Public Safety ("OOPS") is entering this Addendum acting in its capacity as the CJIS Systems Agency (CSA)

for Customer.

3.2 On behalf of all Covered Affiliates, OOPS will perform personnel screening of Google Personnel whose job functions require, in Google's reasonable determination, unescorted, direct logical or physical access to unencrypted CJI to deliver the Covered Services. Google Personnel will also exercise certain other rights or obligations under the CJIS Security Policy as described in this Agreement. For OOPS to perform these functions, Google will provide OOPS information that is proprietary or confidential, including highly sensitive personal information pertaining to Google Personnel. This information will be treated as Google Confidential Information and OOPS will comply with applicable data privacy and security laws.

4. Covered Services. Purchase or use of Covered Services by Customer or an Agency Affiliate will be subject to Customer's or such Agency Affiliate's execution of the GCP Terms (identified in Section 2) with Google, a Google Affiliate, or an Authorized Reseller. Customer and Agency Affiliates obtain no rights or license to use Covered Services under this Addendum.

5. CJIS Requirements.

The CJIS Security Policy applies to Google's provision of Covered Services. Customer and Google have agreed that certain requirements of the CJIS Security Policy will be supported as described in this Section 5.

5.1 CJIS Security Policy Area 2: Security Awareness Training

Google will provide training to all Authorized Google Personnel consistent with CJIS Security Policy part 5.2. Required training will be delivered to applicable personnel within six (6) months of the later of (1) the date a Covered Affiliate first notifies Google it is introducing CJI into the Covered Services, or (2) the date OOPS notifies Google that Google Personnel have passed required Personnel Screening. Google will refresh training for Authorized Google Personnel on at least a biennial basis thereafter.

Google will maintain training records, which will be available to Customer upon written request. Customer will be responsible to provide copies of training records to Agency Affiliates as necessary.

Pursuant to Section 5.2.1 of the CJIS Security Policy, Google employees must complete basic security awareness training conducted via CJIS Online (www.cjisonline.com). This training is tracked via Google's internal HR system and supporting documentation can be provided to the Customer.

5.2 CJIS Security Policy Area 3: Incident Response. In the event of an information security incident affecting the Covered Services, Google will address such incident with Covered Affiliates as described in section 7.2 of the OPST.

5.3. CJIS Security Policy Area 11: Formal Audits

If the Customer or FBI CJIS Division wants to perform an audit of the Covered Services to assess compliance with applicable statutes, regulations, and policies, Google will cooperate with such audit in good faith. Such audits shall be conducted at the sole expense of the auditing entity and will not include access to or examination of data belonging to Google customers in the multi-tenant environment from which the Covered Services are delivered. Access to a Covered Affiliate's data via the Covered Services will be subject to their GCP Terms. If the auditor identifies what it believes to be deficiencies in the Covered Services as a result of an audit, Google and Customer are committed to working together in good faith to resolve the auditor's concerns through discussion and interaction among Customer, Google, and the auditor. Should the participation of a Covered Affiliate be required, Customer will coordinate such participation. Audit information provided by Google to the auditor will be treated as Google Confidential Information accordance with Section 6.

5.4. Policy Area 12: Personnel Security

5.4.a Personnel Screening.

OOPS will be responsible for performing personnel screening (i.e., state and federal fingerprint- based background checks) for applicable Google Personnel under section 5.12 of the CJIS Security Policy.

To facilitate such screening: OOPS will provide Google with the adjudication criteria used by OOPS as may be updated from time to time. Google will provide OOPS a list of Google Personnel anticipated to have unescorted logical access to unencrypted CJI. With respect to Google Personnel in scope for personnel screening, Google will ensure delivery to OOPS of (a) mutually agreed background information, (b) via a mutually agreed mechanism to enable OOPS to perform adjudication.

OOPS will provide Google with confirmation of whether Google Personnel have met the background check criteria and will maintain a list of Authorized Google Personnel. Screening will be performed by the OOPS on behalf of all agencies or entities that may onboard to the Covered Services as Covered Affiliates. Adjudication by Agency Affiliates will not be permitted. OOPS will be responsible for confirming to Covered Affiliates that required personnel screening has been completed and will maintain and provide such records of completed personnel screening to such Covered Affiliates.

5.4.b. Escorted Access. During the Term, Google will maintain a written policy prohibiting unauthorized access by Google Personnel to CJI, and will enforce this through a system by which temporary access to unencrypted CJI is approved, monitored, and tracked for compliance with the CJIS Security Policy. Google uses an escorted access model to control and limit

access to logical and physical unencrypted CJI. If Google Personnel who have not been screened in accordance with section 5.12 of the CJIS Security Policy require access to the Covered Services, Google will ensure such access is supervised by Authorized Google Personnel. Due to the nature of operating a multi-tenant cloud and to maintain the security, continuity and reliability of Google's services, some operations involving (but not limited to) system updates, maintenance, or emergency repairs, may result in incidental unescorted exposure to unencrypted CJI. Google will implement and maintain appropriate security measures in accordance with section 7.1 of the DPST.

5.4.c. If Google reaches agreement with a federal law enforcement agency under which such federal agency conducts personnel screening for the Covered Services in a manner consistent with the requirements of the CJIS Security Policy, OOPS will consider in good faith whether it can rely on such screening in lieu of adjudication by OOPS; and Google and OOPS confirm a mutual desire to develop a scalable screening process that may be leveraged across multiple customers of Covered Services (including those in other states) for whom CJIS compliance is relevant.

6. Confidentiality.

6.1 Confidentiality Obligations. Subject to Section 6.3 (Disclosure of Confidential Information), the recipient will use the other party's Confidential Information only to exercise its rights and fulfill its obligations under the Agreement. The recipient will use reasonable care to protect against disclosure of the other party's Confidential Information to parties other than the recipient's employees, Affiliates, agents, or professional advisors ("Delegates") who need to know it and who have a legal obligation to keep it confidential. The recipient will ensure that its Delegates are also subject to the same non-disclosure and use obligations.

6.2 FOIA. Google acknowledges that the Customer may be subject to and required to comply with a Freedom of Information Act or similar open records or "sunshine" law (collectively "FOIA" laws). If Customer is subject to a FOIA law, Customer will notify Google before releasing any Google Confidential Information to a requester. Unless the law specifies otherwise, Google must receive notice as specified under applicable law or regulation from the Customer before the Customer releases Google Confidential Information. Customer and Covered Affiliates will comply with the CJIS Security Policy when using the Covered Services for all data, including requirements to encrypt data at rest and in transit using encryption keys managed by the Covered Affiliate.

6.3 Disclosure of Confidential Information.

(a) **General.** Regardless of any other provision in the Agreement, and subject to any FOIA law, the recipient and its Delegates may disclose the other party's Confidential Information (i) with the other party's written consent or (ii) in accordance with a Legal Process request, subject to Section 6.3(b) (Legal Process Notification).

(b) **Legal Process Notification.** The recipient will use commercially reasonable efforts to

notify the other party before disclosing that party's Confidential Information in accordance with Legal Process. Notice is not required before disclosure if (i) the recipient is legally prohibited from giving notice or (ii) such notice is impracticable because the Legal Process relates to exceptional circumstances involving danger of death or serious physical injury. Notwithstanding the foregoing and to the extent not legally prohibited, recipient will use commercially reasonable efforts to notify the other party after disclosure.

6.4 Duration of Confidentiality Obligation. Except as permitted above, the parties will not disclose the other party's Confidential Information. This obligation continues for as long as the recipient retains the other party's Confidential Information. Unless required by law to retain Confidential Information, upon termination of this Agreement, each party will delete all Confidential Information received by it under this Agreement.

7. Term.

This Addendum will become effective upon the Effective Date, subject to the termination provisions in this Section 7, this Agreement will automatically terminate upon termination of the last Covered Affiliate's agreement for Covered Services.

8. Miscellaneous.

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

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

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

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

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

8.10 Entire Addendum. The Addendum states all terms agreed between the parties, and supersedes any prior or contemporaneous agreements between the parties relating to the subject matter of the Addendum. In entering into the Addendum, neither party has relied on, and neither party will have any right or remedy based on, any statement, representation, or warranty (whether made negligently or innocently), except those expressly described in the Addendum.

8.11 Conflicting Terms. In the event of conflict between the contract documentation, the documents will control in the following order: (1) the General Terms, and (2) Schedule 1 - Security Addendum.

8.12 Counterparts. The parties may execute the Addendum in counterparts, including facsimile,

PDF, and other electronic copies, which taken together will constitute one instrument.

8.13 Electronic Signatures. The parties consent to electronic signatures.

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



OKLAHOMA
Office of Management
& Enterprise Services

IN WITNESS WHEREOF, the Parties hereby agree to be bound by the terms of this Addendum as indicated by the signatures of their authorized representatives below.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

GOOGLE LLC

By: 
Dan Cronin (Jun 25, 2025 09:45 CDT)

Name: Dan Cronin

Title: State Chief Information Officer

Date: Jun 25, 2025

By:

Name:

Title:

Date:


Philipp Schindler
Authorized Signatory

2025.06.24
09:32:14
-07'00'

SCHEDULE 1

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised.

The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:



HOMA
Office of Management
& Enterprise Services

OKLA

Information Security Officer
Criminal Justice Information Services Division, FBI 1000
Custer Hollow Road
Clarksburg, West Virginia 26306



EXHIBIT

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

This certification is provided for illustrative purposes only; a certification will be executed after the Agreement is executed by Google Personnel with unescorted physical or logical access to unencrypted CJ/.

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Vendor Employee (Printed Name)

Vendor Employee (Signature)

Date

Vendor Representative (Signature)

Date



HOMA
Office of Management
& Enterprise Services

OKLA

Title of Vendor Representative

Company Name

Attachment E3

Google Cloud Master Agreement – Public Sector (Partner)

This Google Cloud Master Agreement is comprised of the Google Cloud Master Agreement General Terms (“General Terms”), and all Services Schedules that are incorporated by reference into the Google Cloud Master Agreement (collectively, the “Agreement”).

Google Cloud Master Agreement General Terms

1. **Services.** After the Customer and Reseller and/or Distributor complete and execute an Order Form incorporating this Agreement; Google will provide the Services specified in the Order Form in accordance with the Agreement, including the SLAs, and Customer and its End Users may use the Services in accordance with the Services Schedule.
2. **Customer Obligations.**
 - 2.1 **Consents.** Customer is responsible for any consents and notices required to permit (a) Customer’s use and receipt of the Services and (b) Google’s accessing, storing, and processing of data provided by Customer (including Customer Data, if applicable) under the Agreement.
 - 2.2 **Compliance.** Customer will (a) ensure that Customer and its End Users’ use of the Services complies with the Agreement, (b) use commercially reasonable efforts to prevent and terminate any unauthorized access or use of the Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Services of which Customer becomes aware.
 - 2.3 **Use Restrictions.** Customer will not, and will not allow End Users to, (a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any of the source code of the Services (except to the extent such restriction is expressly prohibited by applicable law); (b) sell, resell, sublicense, transfer, or distribute the Services; or (c) access or use the Services (i) for High Risk Activities; (ii) in a manner intended to avoid incurring Fees; (iii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (iv) in a manner that breaches, or causes the breach of, Export Control Laws; or (v) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA with Google (if approved), or an executed HIPAA BAA with Google’s Reseller or Distributor.
3. **RESERVED.**
4. **Intellectual Property.**
 - 4.1 **Intellectual Property Rights.** Except as expressly described in the Agreement, the Agreement does not grant either party any rights, implied or otherwise, to the other’s content or Intellectual Property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data and Customer Applications, and Google retains all Intellectual Property Rights in the Services and Software.
 - 4.2 **Feedback.** At its option, Customer may provide feedback and suggestions about the Services to Google (“Feedback”). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer.
5. **Confidentiality.**

- 5.1 **Use and Disclosure of Confidential Information.** The Recipient will only use the Disclosing Party's Confidential Information to exercise its rights and fulfill its obligations under the Agreement, and will use reasonable care to protect against the disclosure of the Disclosing Party's Confidential Information. Notwithstanding any other provision in the Agreement, the Recipient may disclose the Disclosing Party's Confidential Information (a) to its Delegates who have a need to know and who are bound by confidentiality obligations at least as protective as those in this Section 5 (Confidentiality); (b) with the Disclosing Party's written consent; (c) subject to Section 5.2 (Legal Process), as strictly necessary to comply with Legal Process; or (d) in order to comply with the Oklahoma Open Records Act or any other law of the State of Oklahoma or the United States.
- 5.2 **Legal Process.** If the Recipient receives Legal Process for the Disclosing Party's Confidential Information, the Recipient will: (a) promptly notify the Disclosing Party prior to such disclosure unless the Recipient is legally prohibited from doing so; (b) Google will attempt to redirect the third party to request it from the Disclosing Party directly; and (c) use commercially reasonable efforts to object to, or limit or modify, any Legal Process that the Recipient reasonably determines is overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. To facilitate the request in (b), the Recipient may provide the Disclosing Party's basic contact information to the third party. Google acknowledges that the Customer may be subject to and must comply with the Freedom of Information Act (FOIA) or similar Open Records/Sunshine law.
6. **Marketing and Publicity.** Customer may state publicly that it is a Google customer and display Google Brand Features in accordance with the Trademark Guidelines. Upon Customer's written consent (which will not be unreasonably withheld or delayed), Google may use Customer's name and Brand Features in online or offline promotional materials of the Services. Each party may use the other party's Brand Features only as permitted in the Agreement. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features.
7. **Representations and Warranties.** Each party represents and warrants that it (a) has full power and authority to enter into the Agreement and (b) will comply with all laws applicable to its provision, receipt, or use of the Services and TSS, as applicable.
8. **Disclaimer.** Except as expressly provided for in the Agreement, to the fullest extent permitted by applicable law, Google (a) does not make any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, or fitness for a particular use, and (b) makes no representation about content or information accessible through the Services.
9. **Indemnification.**
- 9.1 **Google Indemnification Obligations.** To the extent the Customer seeks indemnification from Google by tendering defense pursuant to this section, Google will defend Customer and its Covered Affiliates, and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that the Google Indemnified Materials used in accordance with the Agreement infringe the third party's Intellectual Property Rights.
- 9.2 **RESERVED.**
- 9.3 **Indemnification Exclusions.** Section 9.1 (Google Indemnification Obligations) will not apply to the extent the underlying allegation arises from (a) the indemnified party's breach of the Agreement or (b) a combination of the Google Indemnified Materials or Customer Indemnified Materials (as applicable) with materials not provided by the indemnifying party under the Agreement, unless the combination is required by the Agreement.

9.4 Indemnification Conditions. Sections 9.1 (Google Indemnification Obligations) are conditioned on the following. Any indemnified party must promptly notify the indemnifying party in writing of any allegation(s) that preceded the Third-Party Legal Proceeding and cooperate reasonably with the indemnifying party to resolve the allegation(s) and Third-Party Legal Proceeding. If breach of this Section 9.4(a) prejudices the defense of the Third-Party Legal Proceeding, the indemnifying party's obligations under Section 9.1 (Google Indemnification Obligations) (as applicable) will be reduced in proportion to the prejudice.

9.5 Remedies.

- (a) If Google reasonably believes the Services might infringe a third party's Intellectual Property Rights, then Google may, at its sole option and expense, (i) procure the right for Customer to continue using the Services, (ii) modify the Services to make them non-infringing without materially reducing their functionality, or (iii) replace the Services with a non-infringing, functionally equivalent alternative.
- (b) If Google does not believe the remedies in Section 9.5(a) are commercially reasonable, then Google may Suspend or terminate the impacted Services. If Google terminates Services under this Section 9.5 (Remedies), then upon Customer request Google will refund to Customer any unused prepaid Fees that Customer paid to Google for use of the terminated Services.

9.6 Sole Rights and Obligations. Without affecting either party's termination or Suspension rights, this Section 9 (Indemnification) states the parties' right to remedy under the Agreement for any third-party allegations of Intellectual Property Rights infringement covered by this Section 9 (Indemnification).

10. Liability.

10.1 Limited Liabilities.

- (a) To the extent permitted by applicable law and subject to Section 10.2 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Agreement for any
 - (i) indirect, consequential, special, incidental, or punitive damages or
 - (ii) lost revenues, profits, savings, or goodwill.
- (b) Google's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the greater of (i) Fees Customer paid for all State of Oklahoma purchases under the applicable Services Schedule during the 12 month period before the event giving rise to Liability; or (ii) \$2,000,000 USD.
- (c) **Enhanced Liability Cap for Security Obligations.** Google's total aggregate Liability for damages arising out of or relating to a Data Incident caused as a direct result of Google's breach of its obligations under the applicable Data Processing and Security Terms and/or State of Oklahoma and Google LLC Agreed Information Security Requirements is limited to \$20,000,000 USD. For sake of clarity, the Enhanced Liability Cap referenced in this section is not a "per claim" or "per event" cap but rather is a maximum cap for all Data Incidents that may arise during the term of the Agreement. Any amount Google pays subject to the Enhanced Liability Cap will reduce the cap applicable to Google in Section 10.1(b), and any amount Google pays subject to the cap in Section 10.1(b) will reduce the Enhanced Liability Cap.

10.2 Unlimited Liabilities. Nothing in the Agreement, to the extent permitted by applicable law, excludes or limits either party's Liability for:

- (a) death, personal injury, or tangible personal property damage resulting from its negligence or the negligence of its employees or agents;**
- (b) its fraud or fraudulent misrepresentation;**
- (c) its obligations under Section 9 (Indemnification);**
- (d) its infringement of the other party's Intellectual Property Rights;**
- (e) its payment obligations under the Agreement; or**
- (f) matters for which liability cannot be excluded or limited under applicable law.**

Notwithstanding the foregoing, Customer's liability is expressly limited by law.

11. Termination.

- 11.1 Agreement Term. The Agreement, unless it expires or terminates according to the Reseller Agreement or Distributor Agreement, will remain in effect for the contract period as described in the applicable Reseller Agreement or Distributor Agreement (the "Term"). For avoidance of doubt, only the Chief Information Officer on behalf of the State of Oklahoma may terminate the Agreement.
- 11.2 Termination for Convenience. Subject to any financial commitments in an Order Form or addendum to the Agreement, Customer may terminate the Agreement or an Order Form for convenience with 30 days' prior written notice to Reseller or Distributor.
- 11.3 Termination for Non-Appropriation. Customer may terminate the Agreement or an Order Form if funds sufficient to pay its obligations under are not appropriated by the applicable state legislature, federal government, or other appropriate government entity, or received from an intended third party funding source. In the event of such insufficiency, Customer shall provide ten (10) calendar days' written notice of intent to terminate. Notwithstanding the foregoing, if Customer issues and order and has accepted the products and/or services under such order, the Customer shall be obligated to pay for such products and/or services.
- 11.4 Effects of Termination. Subject to the Data Processing and Security Terms, Google shall not take any action to intentionally erase any Customer Data. Customer shall be entitled to any post termination or expiration assistance generally made available with respect to the services. If the Agreement terminates, then all Services Schedules and Order Forms also terminate. If an Order Form terminates or expires, then after that Order Form's termination or expiration effective date, (a) all rights and access to the Services under that Order Form will terminate (including access to Customer Data, if applicable), unless otherwise described in the applicable Services Schedule, and (b) Reseller or Distributor will send Customer a final invoice (if applicable) for payment obligations under that Order Form. Termination or expiration of one Order Form will not affect other Order Forms.
- 11.5 Survival. The following Sections will survive expiration or termination of the Agreement: Section 4 (Intellectual Property), Section 5 (Confidentiality), Section 8 (Disclaimer), Section 9 (Indemnification), Section 10 (Liability), Section 11 (Term and Termination), Section 12 (Miscellaneous), Section 13 (Definitions), and any additional sections specified in the applicable Services Schedule.

12. Miscellaneous.

- 12.1 Notices. Under the Agreement, notices to Customer must be sent to the Notification Email and notices to Google must be sent to legal-notices@google.com. Notice will be treated as received when the email

is sent. Customer is responsible for keeping its Notification Email Address current throughout the Term.

- 12.2 Emails. The parties may use emails to satisfy written approval and consent requirements under the Agreement.
- 12.3 Assignment. Neither party may assign the Agreement without the written consent of the other, except to an Affiliate where (a) the assignee has agreed in writing to be bound by the terms of the Agreement, (b) the assigning party has notified the other party of the assignment, and (c) if Customer is the assigning party, the assignee is established in the same country as Customer. Any other attempt to assign is void.
- 12.4 Change of Control. If a party experiences a change of Control other than an internal restructuring or reorganization, then (a) that party will give written notice to the other party within 30 days after the change of Control and (b) the other party may immediately terminate the Agreement any time within 30 days after it receives that written notice.
- 12.5 Force Majeure. Neither party will be liable for failure or delay in performance of its obligations to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war.
- 12.6 Subcontracting. Google may subcontract obligations under the Agreement and will remain liable to Customer for any subcontracted obligations. To the extent Google subcontracts any of its obligations to any third party vendors, contractors, subcontractors, agents, or consultants (collectively, "Subcontractors"), Google will remain liable for all subcontracted obligations and will be responsible for all acts and omissions of such Subcontractors in connection with the Services.
- 12.7 No Agency. The Agreement does not create any agency, partnership, or joint venture between the parties.
- 12.8 No Waiver. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Agreement.
- 12.9 Severability. If any part of the Agreement is invalid, illegal, or unenforceable, the rest of the Agreement will remain in effect.
- 12.10 No Third-Party Beneficiaries. The Agreement does not confer any rights or benefits to any third party unless it expressly states that it does.
- 12.11 Equitable Relief. Nothing in the Agreement will limit either party's ability to seek equitable relief.
- 12.12 RESERVED.
- 12.13 Amendments. Except as specifically described otherwise in the Agreement, any amendment to the Agreement must be in writing, expressly state that it is amending the Agreement, and be signed by Customer and Reseller.
- 12.14 Independent Development. Nothing in the Agreement will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs, or technology that are similar to the subject of the Agreement, provided that the party does not breach its obligations under the Agreement in doing so.
- 12.15 State of Oklahoma and Google LLC Agreed Information Security Requirements. The parties agree that the State of Oklahoma and Google LLC Agreed Information Security Requirements agreement, signed by the State of Oklahoma by and through the Office of Management and Enterprise Services and

Google LLC on March 24, 2022, are incorporated by reference to this Contract as Attachment E2.

- 12.16 Conflicting Terms. Any claim, dispute, or litigation relating to the agreement, in the singular or in the aggregate, shall be governed by the laws of the State of Oklahoma without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma. If there is a conflict among the documents that make up the Agreement, then the documents will control in the following order (of decreasing precedence): State of Oklahoma and Google LLC Agreed Information Security Requirements, the Cloud Master Agreement, the Data Processing and Security Terms, and the other URL Terms. The URL Terms will not expand liability or reduce the rights of the Customer.
- 12.17 Conflicting Languages. If the Agreement is translated into any other language, and there is a discrepancy between the English text and the translated text, the English text will control.
- 12.18 RESERVED.
- 12.19 RESERVED.
- 12.20 Headers. Headings and captions used in the Agreement are for reference purposes only and will not have any effect on the interpretation of the Agreement.
- 12.21 Accessibility. Google agrees to make any Voluntary Product Accessibility Template (“VPAT”) it has available to the Customer for its review, and shall update the VPAT as necessary in order to allow Customer to obtain current VPAT information as required by law.
- 13.** Definitions. The Definitions contained in this section apply only to this Cloud Master Agreement.

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

“AUP” means Google’s acceptable use policy as defined in the applicable Services Schedule (if applicable).

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

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

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

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

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

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

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

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

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

“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. Google will notify Customer promptly and without undue delay, in no case more than 24 hours after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

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

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

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

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

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

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

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

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

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

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

“including” means including but not limited to.

“Indemnified Liabilities” means any (a) settlement amounts approved by the indemnifying party, and (b) damages and costs, including reasonable attorneys’ fees finally awarded against the indemnified party by a court of competent jurisdiction.

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

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

“Legal Process” means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, or other valid legal authority, legal procedure, or similar process.

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

“Notification Email Address” has the meaning described in the applicable Services Schedule.

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

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

“Payment Due Date” means 30 days from the invoice date.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ATTACHMENT E4

Google Cloud Master Agreement Google Cloud Platform Services Schedule

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

1. Using the Services.

- 1.1 Admin Console. Google (or Reseller or Distributor) will provide Customer an Account to access the Admin Console through which Customer may manage its use of the Services. Customer is responsible for (a) maintaining the confidentiality and security of the Account and associated passwords and (b) any use of the Account.
- 1.2 Ceasing Services Use. Customer may stop using the Services at any time.
- 1.3 Customer Applications. Customer may enable End Users to access its Customer Applications.
- 1.4 Additional Use Restrictions. Unless otherwise permitted in the GCP Service Specific Terms, Customer will not (a) use, and will not allow End Users to use, the Services to operate or enable any telecommunications service, or to place or receive calls from any public switched telephone network, including as part of a Customer Application; or (b) use the Services to provide a hosting, outsourced, or managed services solution to unaffiliated third parties, except as part of a Customer Application that provides value distinct from the Services.

2. Data Processing and Security.

- 2.1 Protection of Customer Data. Google will only access or use Customer Data to provide the Services and TSS ordered by Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards to protect Customer Data, as further described in the Data Processing and Security Terms.
- 2.2 Data Processing and Security Terms. The Data Processing and Security Terms are incorporated by reference into this Services Schedule.

3. Additional Payment Terms.

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

3.3 RESERVED.

4. Updates to Services and Terms.

4.1 Changes to Services.

- (a) Limitations on Changes. Google may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services.
- (b) Discontinuance. Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality), and at least 36 months for any Key Service (or associated material functionality), in each case unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.
- (c) Support. Google will continue to provide product and security updates, and GCP Technical Support Services, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).
- (d) Backwards Incompatible Changes. Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner.

4.2 Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing and Security Terms, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms. Notwithstanding the foregoing, negotiated terms between Customer and Google shall supersede any updates from Google unless otherwise mutually agreed by Customer and Google in writing.

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

5. Temporary Suspension.

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

DMS Template ID: 5105795 (v2.7) ~ pg. 10

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

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

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

8. Software.

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

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

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

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

11. Additional Definitions. The Definitions contained in this section apply only to this Cloud Master Agreement.

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

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

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

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

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

"Customer Data" means data provided to Google by Customer or End Users through the

Services under the Account, and data that Customer or End Users derive from that data through their use of the Services.

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

“Data Processing and Security Terms” means the then-current terms describing data processing and security obligations with respect to Customer Data, as described at <https://cloud.google.com/terms/data-processing-terms>.

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

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

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

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

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

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

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

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

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

“Prices” means the then-current applicable prices for the Services or Software described at <https://cloud.google.com/skus/> (incorporated into the Agreement by this reference) unless otherwise agreed in an Order Form or amendment to this Services Schedule.

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

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

“SLA” means the then-current service level agreements described at

<https://cloud.google.com/terms/sla/>.

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

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

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

Attachment E5

Google Cloud Master Agreement Implementation Services Schedule

This Implementation Services Schedule (the “Services Schedule”) supplements and is incorporated by reference into the Google Cloud Master Agreement. This Services Schedule applies to implementation and advisory services described in this Services Schedule that are designed to help Customer use Google products and services. Terms defined in the General Terms apply to this Services Schedule. This Services Schedule is subject to the terms agreed to between Google and the State of Oklahoma in the Google Cloud Master Agreement as well as Attachment A (HIPAA Business Associate Addendum) of the State of Oklahoma and Google LLC Agreed Information Security Requirements. To the extent any of the terms in the Implementation Services Schedule conflict with the Google Cloud Master Agreement and Attachment A (HIPAA Business Associate Addendum) of the State of Oklahoma and Google LLC Agreed Information Security Requirements referenced above, the Google Cloud Master Agreement and Attachment A (HIPAA Business Associate Addendum) of the State of Oklahoma and Google LLC Agreed Information Security Requirements will take precedence.

The parties also agree that none of the Services that Google will provide will include the use of or accessing of State data, including but not limited to, PII or PI. As described in Section 12.6 of the Google Cloud Master Agreement, Google is liable for the acts of any subcontractors used in connection with this Implementation Services Schedule.

1. Services.

- 1.1 Provision of Services. Google will provide Services, including Deliverables, to Customer, subject to Customer fulfilling its obligations under Section 2.1 (Cooperation).
- 1.2 RESERVED.
- 1.3 Invoices and Payment. Customer will pay all Fees, which shall be agreed to in writing, for Services ordered under this Services Schedule. Fees for some Services, to the extent permitted by law, may be non-cancellable, as specified in the Order Form.
- 1.4 Personnel. Google will determine which Personnel will perform the Services. If Customer requests a change of Personnel and provides a reasonable and lawful basis for such request, then Google will use commercially reasonable efforts to replace the assigned Personnel with alternative Personnel.
- 1.5 Compliance with Customer’s Onsite Policies and Procedures. If applicable, Google Personnel performing Services at Customer’s facilities will comply with Customer’s reasonable onsite policies and procedures. Such policies and procedures will be described in an applicable Statement of Work.

2. Customer Obligations.

- 2.1 Cooperation. Customer will provide cooperation in connection with Google’s provision of the Services. Google will not be liable for a delay caused by Customer’s failure to provide Google with the information, materials, consents, or access to Customer facilities, networks, or systems required for Google to perform the Services. If Reseller, Distributor or Google informs Customer of such failure and Customer does not cure the failure within 30 days, then (a) Reseller, Distributor or Google may terminate any incomplete Services and (b) in addition to Fees in Section 6(b) (Effect on Payment).

- 2.2 No Personal Data. Customer acknowledges that Google does not need to process Personal Data to perform the Services. Customer will not provide Google with access to Personal Data unless the parties have agreed in a separate agreement on the scope of work and any terms applicable to Google's processing of such Personal Data. Customer will reimburse expenses as agreed upon by the parties(a) specifically described in the applicable Reseller Order Form; or (b) up to the amounts specified as "expenses" as agreed upon by the parties in the applicable Reseller Order Form or Statement of Work.

3. Intellectual Property.

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

Google Technology. Google owns all rights, title, and interest in Google Technology. To the extent Google Technology is incorporated into Deliverables, Google grants Customer a limited, worldwide, non-exclusive, perpetual, non-transferable license (with the right to sublicense to Affiliates) to use the Google Technology in connection with the Deliverables for Customer's internal business purposes. This Services Schedule does not grant Customer any right to use materials, products, or services that are made available to Google customers under a separate agreement, license, or Services Schedule.

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

4. Warranties and Remedies.

- 4.1 Google Warranty. Google will perform the Services in a professional and workmanlike manner, in accordance with practices used by other service providers performing services similar to the Services. Google will use Personnel with requisite skills, experience, and qualifications to perform the Services.
- 4.2 Remedies. Remedies are addressed in the State of Oklahoma SW1022C Google Cloud Master Agreement (Partner), Section 9.5.

5. RESERVED – TRADE SECRETS.

6. Effects of Termination. If this Services Schedule or an Order Form under this Services Schedule expires or terminates, then:

- (a) Effect on Services. The rights under the Agreement granted by one party to the other regarding the Services will cease immediately except as described in this Section 6 (Effects of Termination), and Google will stop work on the Services.
- (b) Effect on Payment. Subject to rights of termination, Customer will pay for (i) Services, including work-in-progress, performed before the effective date of termination or expiration. Google, Reseller, or Distributor will send Customer a final invoice for payment obligations under the Order Form.

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

7. RESERVED.

8. Additional Definitions.

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

“Covered Affiliate” means an Affiliate receiving the Services under this Services Schedule.

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

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

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

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

“Personal Data” means personal data that: (a) has the meaning given to it in: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“EU GDPR”); or (ii) the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force (“UK GDPR”), as applicable; and (b) would cause Google to be subject to the EU GDPR or the UK GDPR (as applicable) as a data processor for Customer.

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

“Prices” means the amounts agreed to in an Order Form under this Services Schedule.

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



ATTACHMENT E6

GOOGLE CLOUD PROFESSIONAL SERVICES (PSO) SOW

The Google Cloud Professional Services (PSO) SOW is hereby amended as set forth below and supersedes all prior documents submitted by Google or discussed by the parties. The parties agree to use this Google Cloud Professional Services (PSO) SOW or a document substantially similar in the form of this Google Cloud Professional Services (PSO) SOW.

Google Cloud Professional Services (PSO) Statement of Work (Accompanies Professional Services / Implementation Services Order Form)

All gray text is part of the approved Order Form/SOW template.

Customer	{Customer legal name}
SOW Engagement Name	{Engagement name}
SOW ID	b/{buganizer number}
Vector Quote ID	{Quote Q - ID}
SOW Written Date	{Date of Draft SOW}
SOW Scope Validity	SOW scope valid if the Order Form is signed within 60 days of the SOW Written Date.

1. Background

Customer has provided the following information as context for this Statement of Work.

{insert high level Customer requirements}

2. Services

Google will perform the following activities for the Services under this SOW:

- {Activity 1 (start each bullet with an action verb)}
- {Activity 2 (start each bullet with an action verb)}
- {Activity 3 (start each bullet with an action verb)}

Google will not perform the following activities:

{select correct one - if activity based: Delivery of the Services will occur over a period of up to {X} months. If time based: Delivery of the Services will occur over a period of {X} months.}



Requests for Services or development work outside those outlined in Section 2 or delays in Customer activities as described in Section 5 may result in delays and may increase the amount charged for the work described in this SOW.

3. Deliverables

Google will provide the following Deliverables to the Customer under this SOW:

Deliverable	Description/Acceptance Criteria
{Deliverable 1 (must be a noun).}	{Add a descriptive sentence if the name is not obvious. Make sure the description is objective, not subjective ("functioning system")}
{Deliverable 2 (must be a noun).}	{Add a descriptive sentence if the name is not obvious. Make sure the description is objective, not subjective ("functioning system")}

4. Proposed Engagement Staffing

Refer to the governing terms for how Google staffs Personnel to projects.

Under this SOW, Google may staff the following roles. A team member may perform one or more roles. Google may substitute and change actual team members, depending on schedule and availability.

Role	Role Description
Google Cloud Consultant	Primary point of contact between Customer and Google for the engagement
Google Cloud Engineer	Provides supplemental technical expertise in architectural decisions
Google Cloud Subcontracted Engineer	Provides supplemental technical expertise in architectural decisions
Google Cloud Program Manager	Provides engagement project management

Under this SOW, Customer may assign the following roles to the engagement:

Role	Role Description
Customer Sponsor	Customer executive responsible for all Customer approvals



Customer Point of Contact (POC)	Primary Customer contact, responsible for all engagement -related issues
Customer Architect	Customer contact who has authority to make all architectural decisions
Customer Staff	Customer contact who will work day -to-day with Google team members

5. Project Requirements, Ongoing Customer Responsibilities, and Assumptions

Customer acknowledges that Google does not need to process Personal Data to perform the Services, nor will Google perform work in a live production environment. [OPTION 2 PII] Customer acknowledges that Google will not perform work in a live production environment. However, Google may process Customer Personal Data, which will be processed exclusively within a Customer-Managed System (both as defined in the CDPA), whether directly or through its subcontractors. The Cloud Data Processing Addendum available at: <https://cloud.google.com/terms/data-processing-addendum/> (the "CDPA") and Section 7 of this SOW will apply to processing of Customer Personal Data by Google Personnel.

Customer will meet all of the following project prerequisites BEFORE Google will start the Services:

- {Activity 1 (start each bullet with an action verb)}
- {Activity 2 (start each bullet with an action verb)}

Customer will perform the following ONGOING activities during the engagement:

- {Activity 1 (start each bullet with an action verb)}
- {Activity 2 (start each bullet with an action verb)}

The effort estimation and pricing for the work scoped in this SOW is predicated upon the following assumptions. Any changes to these assumptions provided by Customer may impact the scoped pricing or schedule and result in a Change Request:

- {Assumption 1. A critical PSO position which the scope effort and timeline estimations are dependent upon that either needs to be confirmed or regularly reconfirmed during the engagement, and if the position no longer holds true will impact the delivery schedule or cost.}
- {Assumption 2}
- {Assumption 3}

Checkpoints will be conducted {select one: on a weekly basis, on a monthly basis, midway, regularly} during the engagement to reconfirm the assumptions.



6. Fees

Refer to the Order Form for Fees. The following amount shown is a placeholder until the final Order Form is created. The total amount shown below should match the final executed Order Form. If any discrepancies arise in the total amount, the signed Order Form will prevail.

Amount	{XX}
Adjustment	{SXX} {Select one: Credits Redemption or Discount/BIF. Or if no adjustment, delete the first 2 rows}
TOTAL	{XX}

If applicable and for illustration purposes only, details on phases and milestones are shown below. Note: If any discrepancies arise between the Fees, phases, or milestones listed in this section and the final executed Order Form, the signed Order Form will prevail.

Fees Breakdown

Phase/Milestone	Sub Total
{Phase or Milestone}	{Amount}
{Phase or Milestone}	{Amount}
{Phase or Milestone}	{Amount}
{Phase or Milestone}	{Amount}
TOTAL	

The following section (section 7) only applies when the project includes exposure to (including access, and handling of) Personally Identifiable Information (PII) data

7. Additional Security Measures

In addition to the obligations contained in the DPA, Customer agrees to the following additional security measures:

- During onboarding, Google will notify Personnel performing the Services subject to the DPA (“DPA Personnel”) that they will be processing Customer Personal Data (as defined in the DPA).
- Google will remind DPA Personnel of their confidentiality obligations and that Customer Personal Data may only be used to provide the Services described in this SOW.
- Google will only access and process Customer Personal Data in a Google Cloud Platform Account owned and controlled by Customer.
- Google may process the following types of Customer Personal Data for the purpose of performing the Services in this SOW:
 - List data types



8. General Statement of Work Terms

Governing Terms from Order Form	Oklahoma Statewide Contract No. 1041
SOW Start Date	{Start Date}
SOW End Date	{End Date, or X weeks/months after start date }
SOW Effective Dates	The SOW is effective on the last signature date on the SOW and remains in effect until the earlier of (a) the SOW End Date, or (b) the end of the Acceptance Process for the final Deliverable to be provided in this SOW. If additional time or resources are required to complete work, the project may be extended via Change Order (See "Change Request Process" below).
Change Request Process	Either party may request a material modification to the Services in this SOW by submitting a change request to the other party ("Change Request"). Upon receipt of a Change Request, Google may propose additional Fees and adjustments to delivery dates if the Change Request adds scope, time or team members to the Services. The parties will have thirty(30) business days after the Change Request is submitted to agree to amend this SOW, or execute a new Order Form, with a change order executed by the parties; otherwise, the Change Request will be considered withdrawn.
Acceptance Process for Deliverables	1. Customer will have five (5) business days ("First Review Period") following receipt of a Deliverable from Google to determine whether the Deliverable meets specific objective conditions described in this SOW ("Acceptance Criteria"). If Customer provides notice of non-conformity in accordance with Section 2 of this Acceptance Process, Customer will have up to two additional review periods of three (3) business days ("Second Review Period") and three (3) business days ("Third Review Period"), as applicable following receipt of a corrected Deliverable to confirm that the corrected Deliverable meets the applicable Acceptance Criteria. 2. If Customer reasonably determines that a Deliverable does not conform to its Acceptance Criteria, then before the end of the applicable Review Period, Customer will provide written notice to Google describing in detail the nature of the non -conformity. If Customer does not provide notice of acceptance or non -conformity during the applicable Review Period, the Deliverable will be deemed accepted by the Customer. 3. If Customer provides notice of non -conformity in accordance with Section 2 of this Acceptance Process for the First Review Period or Second Review Period, Google will, at no additional cost to the Customer, promptly make any changes reasonably required to correct the non -conformity described in the notice. Google will deliver the corrected Deliverable to the Customer. 4. If Customer provides notice of non -conformity in accordance with Section 2 of this Acceptance Process for the Third Review Period, then unless the Parties agree otherwise in writing, Google will either, as applicable, (i) reduce any unpaid Fees by the amount due for the non-conforming Deliverable or (ii) return Fees in the amount paid for the non -conforming Deliverable, the portion of the Order Form applicable to the Deliverable will terminate, and Customer's license to use the Deliverable will terminate .

ATTACHMENT E7

Google Workspace Services Schedule

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

1. Using the Services.

1.1 Account; Admin Console. Google will provide Customer with an Account that Customer may use to access the Admin Console. Customer may use the Admin Console to specify one or more Administrators to manage Customer’s use of the Services. Customer is responsible for (a) maintaining the confidentiality and security of the Account (including End User Accounts) and associated passwords and (b) any use of the Account (including End User Accounts). Customer agrees that Google’s responsibilities do not extend to the internal management or administration of the Services for Customer.

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

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

2. Data Processing and Security. Google will only access, use, and otherwise process Customer Data in accordance with the terms of this Contract and 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.

3. Additional Payment Terms.

3.1 Usage and Invoicing. Customer will pay all Fees for the Services. Google’s measurement tools will be used to determine Customer’s usage of the Services. Unless otherwise provided in the Agreement or required by law

3.2 Reserved.

4. Updates to Services and Terms.

4.1 Changes to Services.

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

(b) Discontinuance. Notwithstanding Section 4.1(a) (Limitations on Changes), Google may discontinue a Service (or associated material functionality), provided that Google will notify Customer at least 36 months before discontinuing any Key Service (or associated material functionality), and at least 12 months before discontinuing any other Core Service (or associated material functionality), in each case unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

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

4.2 **Changes to Terms**. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Cloud Data Processing Addendum, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material changes to the URL Terms. Material changes to the URL Terms will be effective 30 days after Customer receives notice of such changes.

4.3 **Permitted Changes**. Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to new or pre-general availability Services, offerings, or functionality. Notwithstanding Section 4.2 (Changes to Terms), material changes to the URL Terms made to comply with applicable law or to address a material security risk will be effective upon notice.

5. **Temporary Suspension**.

5.1 **Services Suspension**. Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Customer or any End User's use of the Services does not comply with the AUP, and it is not cured following notice from Google. For Suspensions of End User Accounts, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

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

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

7. **Copyright**. Google responds to notices of alleged copyright infringement and terminates the End User 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.

8. **Additional Customer Responsibilities**.

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

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

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

10. **Additional Products**. Google makes optional Additional Products available to Customer and its End Users. Customer's use of Additional Products is subject to the Additional Product Terms, which are incorporated by reference into this Services Schedule.

12. **Termination of Previous Agreements**. If Google and Customer have previously entered into another agreement under which Customer uses the Services, then that agreement will terminate on the Services Start Date, and the Agreement will govern the provision and use of the Services going forward.

13. **Additional Definitions**.

"Account" means Customer's Google Workspace account.

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

"Additional Product Terms" means the then-current terms at https://workspace.google.com/terms/additional_services.html, as may be updated by Google from time to time.

"Admin Account" means a type of End User Account configured to allow administration of the Services.

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

"Administrator" means the Customer-designated personnel (including Reseller, if applicable) with access to an Admin Account and the ability to access End User Accounts. Such access to End User Accounts includes the ability to access, monitor, use, modify, withhold, or disclose any data available to End Users associated with their End User Accounts.

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

"Cloud Data Processing Addendum" 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>.

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

"Covered Affiliate" means a Customer Affiliate that uses the Services under the Agreement.

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

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

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

"Data Processing Terms" means the Cloud Data Processing Addendum.

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

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

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

“Google Workspace Service Specific Terms” means the then-current terms specific to one or more Services, at <https://workspace.google.com/terms/service-terms/>.

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

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

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

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

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

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

“Prices” means the applicable prices at <https://workspace.google.com/pricing.html> (incorporated into the Agreement by this reference), unless otherwise agreed in an Order Form or amendment to this Services Schedule.

“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 the Agreement.

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

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

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

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

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

“URL Terms” means the AUP, Cloud Data Processing Addendum, Google Workspace Service Specific Terms, Google Workspace Technical Support Services Guidelines, and SLAs. The URL Terms for Google Workspace Services are all available at g.co/cloud/workspace-directory-terms.

PESA_Oklahoma Office of Management Enterprise Services - GCP - Custom Contract 2025_6_24 3.0_

Final Audit Report

2025-06-25

Created:	2025-06-25
By:	Courtney Templeton (courtney.templeton@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAARV4u_tywqFmvv_rmiRex8zCSIEUQrr0v

"PESA_Oklahoma Office of Management Enterprise Services - GCP - Custom Contract 2025_6_24 3.0_" History

-  Document digitally presigned by Dalam Ton (dalamt@google.com)
2025-06-24 - 4:31:34 PM GMT
-  Document digitally presigned by Dalam Ton (dalamt@google.com)
2025-06-24 - 4:32:01 PM GMT
-  Document digitally presigned by Dalam Ton (dalamt@google.com)
2025-06-24 - 4:32:14 PM GMT
-  Document created by Courtney Templeton (courtney.templeton@omes.ok.gov)
2025-06-25 - 2:29:01 PM GMT
-  Document emailed to Dan Cronin (dan.cronin@omes.ok.gov) for signature
2025-06-25 - 2:31:56 PM GMT
-  Email viewed by Dan Cronin (dan.cronin@omes.ok.gov)
2025-06-25 - 2:44:12 PM GMT
-  Document e-signed by Dan Cronin (dan.cronin@omes.ok.gov)
Signature Date: 2025-06-25 - 2:45:16 PM GMT - Time Source: server
-  Agreement completed.
2025-06-25 - 2:45:16 PM GMT