

Agreement No. 30000-24-R_____

AGREEMENT BETWEEN THE COUNTY OF SAN MATEO AND CDW-G

This Agreement is entered into this 15th day of December, 2023, by and between the County of San Mateo, a political subdivision of the state of California, hereinafter called "County," and CDW-G, hereinafter called "Contractor."

* * *

This SOW shall be governed by that certain City of Mesa Agreement Number 2018011 Information Technology Solutions & Services between CDW Government LLC and City of Mesa, Arizona, administered by National IPA, effective March 1, 2018 (the "Agreement"). If there is a conflict between this SOW and the Agreement, then the Agreement will control, except as expressly amended in this SOW by specific reference to the Agreement..

Whereas, pursuant to Section 31000 of the California Government Code, County may contract with independent contractors for the furnishing of such services to or for County or any Department thereof; and

Whereas, it is necessary and desirable that Contractor be retained for the purpose of to providing host and support core applications and solutions in the Amazon Web Services (AWS) government cloud platform.

Now, therefore, it is agreed by the parties to this Agreement as follows:

1. Exhibits and Attachments

The following exhibits and attachments are attached to this Agreement and incorporated into this Agreement by this reference:

Exhibit A – Private Pricing Agreement
 Exhibit B – AWS Cloud Services Addendum
 Exhibit C – Security Standards
 Attachment I—Contract Sanction Letter

2. Services to be performed by Contractor

In consideration of the payments set forth in this Agreement, Contractor shall perform services for County in accordance with the terms, conditions, and specifications set forth in this Agreement and in Exhibit A.

The Parties further acknowledge that the terms and conditions of the [Cloud Services AWS Addendum\(s\)](#) for shall govern with respect to specific Cloud Services. If there is a conflict between the SOW, Agreement and Cloud Services Addendum(s), then the Addendum(s) will control.

Reference to "Cloud" includes AWS and "Cloud Provider" refers to AWS, respectively.

1. The Section entitled Assumptions is amended to include the following:

Native AWS security tools i.e. Identity and Access Management, Guard Duty, etc. can be made available to customer.

2. The Section entitled Service Fees is amended to include Cloud Service Fees outlined as follows:

3. Cloud Service Fees

Customer will pay all Cloud Services Fees monthly, in arrears, based on Customer's actual usage in the

preceding month. Pricing will be based on the pricing effective during the current billing cycle. Seller reserves the right to increase the price that it charges Customer for the Cloud Services in response to increases made by AWS, provided that Seller will provide Customer not less than thirty (30) days prior notice of any such increase.

Notwithstanding the foregoing, the Cloud Services Fees that pertain to AWS Web Services shall also be subject to the additional terms and conditions set forth in the Private Pricing Addendum terms between and between the parties attached hereto as Exhibit A.

4. **Payments**

In consideration of the services provided by Contractor in accordance with all terms, conditions, and specifications set forth in this Agreement and in Exhibit A, County shall make payment to Contractor based on the rates and in the manner specified in Exhibit B. County reserves the right to withhold payment if County determines that the quantity or quality of the work performed is unacceptable. In no event shall County's total fiscal obligation under this Agreement exceed **One Million Five Hundred Thousand Dollars (\$1,500,000.00)**. In the event that the County makes any advance payments, Contractor agrees to refund any amounts in excess of the amount owed by the County at the time of contract termination or expiration. Contractor is not entitled to payment for work not performed as required by this agreement.

5. **Term**

Subject to compliance with all terms and conditions, the term of this Agreement shall be from **April 14, 2023, through April 13, 2028**.

6. **Termination**

This Agreement may be terminated by Contractor or by the Sheriff or Sheriff's designee at any time without a requirement of good cause upon thirty (30) days' advance written notice to the other party. Subject to availability of funding, Contractor shall be entitled to receive payment for work/services provided prior to termination of the Agreement. Such payment shall be that prorated portion of the full payment determined by comparing the work/services actually completed to the work/services required by the Agreement.

County may terminate this Agreement or a portion of the services referenced in the Attachments and Exhibits based upon the unavailability of Federal, State, or County funds by providing written notice to Contractor as soon as is reasonably possible after County learns of said unavailability of outside funding.

County may terminate this Agreement for cause. In order to terminate for cause, County must first give Contractor notice of the alleged breach. Contractor shall have five business days after receipt of such notice to respond and a total of ten calendar days after receipt of such notice to cure the alleged breach. If Contractor fails to cure the breach within this period, County may immediately terminate this Agreement without further action. The option available in this paragraph is separate from the ability to terminate without cause with appropriate notice described above. In the event that County provides notice of an alleged breach pursuant to this section, County may, in extreme circumstances, immediately suspend performance of services and payment under this Agreement pending the resolution of the process described in this paragraph. County has sole discretion to determine what constitutes an extreme circumstance for purposes of this paragraph, and County shall use reasonable judgment in making that determination.

7. Contract Materials

At the end of this Agreement, or in the event of termination, all finished or unfinished documents, data, studies, maps, photographs, reports, and other written materials (collectively referred to as "contract materials") prepared by Contractor under this Agreement shall become the property of County and shall be promptly delivered to County. Upon termination, Contractor may make and retain a copy of such contract materials if permitted by law.

8. Relationship of Parties

Contractor agrees and understands that the work/services performed under this Agreement are performed as an independent contractor and not as an employee of County and that neither Contractor nor its employees acquire any of the rights, privileges, powers, or advantages of County employees.

9. Hold Harmless

a. General Hold Harmless

Contractor shall indemnify and save harmless County and its officers, agents, employees, and servants from all claims, suits, or actions of every name, kind, and description resulting from this Agreement, the performance of any work or services required of Contractor under this Agreement, or payments made pursuant to this Agreement brought for, or on account of, any of the following:

(A) injuries to or death of any person, including Contractor or its employees/officers/agents;

(B) damage to any property of any kind whatsoever and to whomsoever belonging;

(C) any sanctions, penalties, or claims of damages resulting from Contractor's failure to comply, if applicable, with the requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all Federal regulations promulgated thereunder, as amended; or

(D) any other loss or cost, including but not limited to that caused by the concurrent active or passive negligence of County and/or its officers, agents, employees, or servants. However, Contractor's duty to indemnify and save harmless under this Section shall not apply to injuries or damage for which County has been found in a court of competent jurisdiction to be solely liable by reason of its own negligence or willful misconduct.

The duty of Contractor to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

b. Intellectual Property Indemnification

Contractor hereby certifies that it owns, controls, and/or licenses and retains all right, title, and/or interest in and to any intellectual property it uses in relation to this Agreement, including the design, look, feel, features, source code, content, and/or other technology relating to any part of the services it provides under this Agreement and including all related patents, inventions, trademarks, and copyrights, all applications therefor, and all trade names, service marks, know how, and trade secrets (collectively referred to as "IP Rights") except as otherwise noted by this Agreement.

Contractor warrants that the services it provides under this Agreement do not infringe, violate, trespass, or constitute the unauthorized use or misappropriation of any IP Rights of any third party. Contractor shall defend, indemnify, and hold harmless County from and against all liabilities, costs, damages, losses, and expenses (including reasonable attorney fees) arising out of or related to any claim by a third party

that the services provided under this Agreement infringe or violate any third-party's IP Rights provided any such right is enforceable in the United States. Contractor's duty to defend, indemnify, and hold harmless under this Section applies only provided that: (a) County notifies Contractor promptly in writing of any notice of any such third-party claim; (b) County cooperates with Contractor, at Contractor's expense, in all reasonable respects in connection with the investigation and defense of any such third-party claim; (c) Contractor retains sole control of the defense of any action on any such claim and all negotiations for its settlement or compromise (provided Contractor shall not have the right to settle any criminal action, suit, or proceeding without County's prior written consent, not to be unreasonably withheld, and provided further that any settlement permitted under this Section shall not impose any financial or other obligation on County, impair any right of County, or contain any stipulation, admission, or acknowledgement of wrongdoing on the part of County without County's prior written consent, not to be unreasonably withheld); and (d) should services under this Agreement become, or in Contractor's opinion be likely to become, the subject of such a claim, or in the event such a third party claim or threatened claim causes County's reasonable use of the services under this Agreement to be seriously endangered or disrupted, Contractor shall, at Contractor's option and expense, either: (i) procure for County the right to continue using the services without infringement or (ii) replace or modify the services so that they become non-infringing but remain functionally equivalent.

Notwithstanding anything in this Section to the contrary, Contractor will have no obligation or liability to County under this Section to the extent any otherwise covered claim is based upon: (a) any aspects of the services under this Agreement which have been modified by or for County (other than modification performed by, or at the direction of, Contractor) in such a way as to cause the alleged infringement at issue; and/or (b) any aspects of the services under this Agreement which have been used by County in a manner prohibited by this Agreement.

The duty of Contractor to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

10. Assignability and Subcontracting

Contractor shall not assign this Agreement or any portion of it to a third party or subcontract with a third party to provide services required by Contractor under this Agreement without the prior written consent of County. Any such assignment or subcontract without County's prior written consent shall give County the right to automatically and immediately terminate this Agreement without penalty or advance notice.

11. Insurance

c. General Requirements

Contractor shall not commence work or be required to commence work under this Agreement unless and until all insurance required under this Section has been obtained and such insurance has been approved by County's Risk Management, and Contractor shall use diligence to obtain such insurance and to obtain such approval. Contractor shall furnish County with certificates of insurance evidencing the required coverage, and there shall be a specific contractual liability endorsement extending Contractor's coverage to include the contractual liability assumed by Contractor pursuant to this Agreement. These certificates shall specify or be endorsed to provide that thirty (30) days' notice must be given, in writing, to County of any pending change in the limits of liability or of any cancellation or modification of the policy.

d. Workers' Compensation and Employer's Liability Insurance

Contractor shall have in effect during the entire term of this Agreement workers' compensation and employer's liability insurance providing full statutory coverage. In signing this Agreement, Contractor certifies, as required by Section 1861 of the California Labor Code, that (a) it is aware of the provisions of County of San Mateo I CDW-G

Section 3700 of the California Labor Code, which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of the Labor Code, and (b) it will comply with such provisions before commencing the performance of work under this Agreement.

e. Liability Insurance

Contractor shall take out and maintain during the term of this Agreement such bodily injury liability and property damage liability insurance as shall protect Contractor and all of its employees/officers/agents while performing work covered by this Agreement from any and all claims for damages for bodily injury, including accidental death, as well as any and all claims for property damage which may arise from Contractor's operations under this Agreement, whether such operations be by Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or an agent of either of them. Such insurance shall be combined single limit bodily injury and property damage for each occurrence and shall not be less than the amounts specified below:

(a) Comprehensive General Liability.....	\$1,000,000
(b) Motor Vehicle Liability Insurance.....	\$1,000,000
(c) Professional Liability.....	\$1,000,000

County and its officers, agents, employees, and servants shall be named as additional insured on any such policies of insurance, which shall also contain a provision that (a) the insurance afforded thereby to County and its officers, agents, employees, and servants shall be primary insurance to the full limits of liability of the policy and (b) if the County or its officers, agents, employees, and servants have other insurance against the loss covered by such a policy, such other insurance shall be excess insurance only.

In the event of the breach of any provision of this Section, or in the event any notice is received which indicates any required insurance coverage will be diminished or canceled, County, at its option, may, notwithstanding any other provision of this Agreement to the contrary, immediately declare a material breach of this Agreement and suspend all further work and payment pursuant to this Agreement.

12. Compliance With Laws

All services to be performed by Contractor pursuant to this Agreement shall be performed in accordance with all applicable Federal, State, County, and municipal laws, ordinances, regulations, and executive orders, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Regulations promulgated thereunder, as amended (if applicable), the Business Associate requirements set forth in Attachment H (if attached), the Americans with Disabilities Act of 1990, as amended, and Section 504 of the Rehabilitation Act of 1973, which prohibits discrimination on the basis of disability in programs and activities receiving any Federal or County financial assistance, as well as any required economic or other sanctions imposed by the United States government or under state law in effect during the term of the Agreement. Such services shall also be performed in accordance with all applicable ordinances and regulations, including but not limited to appropriate licensure, certification regulations, provisions pertaining to confidentiality of records, and applicable quality assurance regulations. In the event of a conflict between the terms of this Agreement and any applicable State, Federal, County, or municipal law, regulation, or executive order, the requirements of the applicable law, regulation, or executive order will take precedence over the requirements set forth in this Agreement.

Chapter 4.107 of the San Mateo County Ordinance Code, which regulates the use of disposable food service ware. Accordingly, Contractor shall not use any non-recyclable plastic disposable food service ware when providing prepared food on property owned or leased by the County and instead shall use biodegradable, compostable, reusable, or recyclable plastic food service ware on property owned or leased by the County.

Contractor will timely and accurately complete, sign, and submit all necessary documentation of compliance.

13. Non-Discrimination and Other Requirements

a. General Non-discrimination

No person shall be denied any services provided pursuant to this Agreement (except as limited by the scope of services) on the grounds of race, color, national origin, ancestry, age, disability (physical or mental), sex, sexual orientation, gender identity, marital or domestic partner status, religion, political beliefs or affiliation, familial or parental status (including pregnancy), medical condition (cancer-related), military service, or genetic information.

b. Equal Employment Opportunity

Contractor shall ensure equal employment opportunity based on objective standards of recruitment, classification, selection, promotion, compensation, performance evaluation, and management relations for all employees under this Agreement. Contractor's equal employment policies shall be made available to County upon request.

c. Section 504 of the Rehabilitation Act of 1973

Contractor shall comply with Section 504 of the Rehabilitation Act of 1973, as amended, which provides that no otherwise qualified individual with a disability shall, solely by reason of a disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination in the performance of any services this Agreement. This Section applies only to contractors who are providing services to members of the public under this Agreement.

d. Compliance with County's Equal Benefits Ordinance

Contractor shall comply with all laws relating to the provision of benefits to its employees and their spouses or domestic partners, including, but not limited to, such laws prohibiting discrimination in the provision of such benefits on the basis that the spouse or domestic partner of the Contractor's employee is of the same or opposite sex as the employee.

e. Discrimination Against Individuals with Disabilities

The nondiscrimination requirements of 41 C.F.R. 60-741.5(a) are incorporated into this Agreement as if fully set forth here, and Contractor and any subcontractor shall abide by the requirements of 41 C.F.R. 60-741.5(a). This regulation prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified individuals with disabilities.

f. History of Discrimination

Contractor certifies that no finding of discrimination has been issued in the past 365 days against Contractor by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other investigative entity. If any finding(s) of discrimination have been issued against Contractor within the past 365 days by the Equal Employment Opportunity Commission, County of San Mateo I CDW-G

the California Department of Fair Employment and Housing, or other investigative entity, Contractor shall provide County with a written explanation of the outcome(s) or remedy for the discrimination prior to execution of this Agreement. Failure to comply with this Section shall constitute a material breach of this Agreement and subjects the Agreement to immediate termination at the sole option of the County.

g. Reporting: Violation of Non-discrimination Provisions

Contractor shall also report to the County the filing by any person in any court any complaint of discrimination or the filing by any person of any and all charges with the Equal Employment Opportunity Commission, the Fair Employment and Housing Commission, or any other entity charged with the investigation of allegations of discrimination within seventy-five (75) days of such filing, provided that within such seventy-five (75) days such entity has not notified contractor that such charges are dismissed or otherwise unfounded. Such notification to County shall include a general description of the allegations and the nature of specific claims being asserted. Contractor shall provide County with a statement regarding how it responded to the allegations within sixty (60) days of its response and shall update County regarding the nature of the final resolution of such allegations.

Violation of the non-discrimination provisions of this Agreement shall be considered a breach of this Agreement and subject the Contractor to penalties, to be determined by the County Executive Officer, including but not limited to the following:

- i. termination of this Agreement;
- ii. disqualification of the Contractor from being considered for or being awarded a County contract for a period of up to 3 years;
- iii. liquidated damages of \$2,500 per violation; and/or
- iv. imposition of other appropriate contractual and civil remedies and sanctions, as determined by the County Executive Officer.

To effectuate the provisions of this Section, the County Executive shall have the authority to offset all or any portion of the amount described in this Section against amounts due to Contractor under this Agreement or any other agreement between Contractor and County.

h. Compliance with Living Wage Ordinance

As required by Chapter 2.88 of the San Mateo County Ordinance Code, Contractor certifies all contractor(s) and subcontractor(s) obligated under this contract shall fully comply with the provisions of the County of San Mateo Living Wage Ordinance, including, but not limited to, paying all Covered Employees the current Living Wage and providing notice to all Covered Employees and Subcontractors as required under the Ordinance.

14. Compliance with County Employee Jury Service Ordinance

Contractor shall comply with Chapter 2.85 of the County's Ordinance Code, which states that Contractor shall have and adhere to a written policy providing that its employees, to the extent they are full-time employees and live in San Mateo County, shall receive from the Contractor, on an annual basis, no fewer than five days of regular pay for jury service in San Mateo County, with jury pay being provided only for each day of actual jury service. The policy may provide that such employees deposit any fees received for such jury service with Contractor or that the Contractor may deduct from an employee's regular pay the fees received for jury service in San Mateo County. By signing this Agreement, Contractor certifies that it has and adheres to a policy consistent with Chapter 2.85. For purposes of this Section, if Contractor has no employees in San Mateo County, it is sufficient for Contractor to provide the following written statement to County: "For purposes of San Mateo County's jury service ordinance, Contractor certifies that it has no full-time employees who live in San Mateo County. To the extent that it hires any

such employees during the term of its Agreement with San Mateo County, Contractor shall adopt a policy that complies with Chapter 2.85 of the County's Ordinance Code." The requirements of Chapter 2.85 do not apply unless this Agreement's total value listed in the Section titled "Payments", exceeds two-hundred thousand dollars (\$200,000); Contractor acknowledges that Chapter 2.85's requirements will apply if this Agreement is amended such that its total value exceeds that threshold amount.

15. Retention of Records: Right to Monitor and Audit

(a) Contractor shall maintain all required records relating to services provided under this Agreement for three (3) years after County makes final payment and all other pending matters are closed, and Contractor shall be subject to the examination and/or audit by County, a Federal grantor agency, and the State of California.

(b) Contractor shall comply with all program and fiscal reporting requirements set forth by applicable Federal, State, and local agencies and as required by County.

(c) Contractor agrees upon reasonable notice to provide to County, to any Federal or State department having monitoring or review authority, to County's authorized representative, and/or to any of their respective audit agencies access to and the right to examine all records and documents necessary to determine compliance with relevant Federal, State, and local statutes, rules, and regulations, to determine compliance with this Agreement, and to evaluate the quality, appropriateness, and timeliness of services performed.

16. Merger Clause: Amendments

This Agreement, including the Exhibits and Attachments attached to this Agreement and incorporated by reference, constitutes the sole Agreement of the parties to this Agreement and correctly states the rights, duties, and obligations of each party as of this document's date. In the event that any term, condition, provision, requirement, or specification set forth in the body of this Agreement conflicts with or is inconsistent with any term, condition, provision, requirement, or specification in any Exhibit and/or Attachment to this Agreement, the provisions of the body of the Agreement shall prevail. Any prior agreement, promises, negotiations, or representations between the parties not expressly stated in this document are not binding. All subsequent modifications or amendments shall be in writing and signed by the parties.

17. Controlling Law: Venue

The validity of this Agreement and of its terms, the rights and duties of the parties under this Agreement, the interpretation of this Agreement, the performance of this Agreement, and any other dispute of any nature arising out of this Agreement shall be governed by the laws of the State of California without regard to its choice of law or conflict of law rules. Any dispute arising out of this Agreement shall be venued either in the San Mateo County Superior Court or in the United States District Court for the Northern District of California.

18. Notices

Any notice, request, demand, or other communication required or permitted under this Agreement shall be deemed to be properly given when both: (1) transmitted via email to the email address listed below; and (2) sent to the physical address listed below by either being deposited in the United States mail, postage prepaid, or deposited for overnight delivery, charges prepaid, with an established overnight courier that provides a tracking number showing confirmation of receipt.

In the case of County, to:

Name/Title: Veronica Ruiz/Management Analyst
Address: 400 County Center, 3rd floor, Redwood City, CA 94063
Telephone: 650-363-7819
Email: VRuiz@smcgov.org

In the case of Contractor, to:

Name/Title: Chris Schroeder/Manager, Services Contracts
Address: 200 N. Milwaukee Avenue, Vernon Hills, IL 60062
Telephone: 800-800-4239
Email: chschro@cdw.com

19. Electronic Signature

Both County and Contractor wish to permit this Agreement and future documents relating to this Agreement to be digitally signed in accordance with California law and County's Electronic Signature Administrative Memo. Any party to this Agreement may revoke such agreement to permit electronic signatures at any time in relation to all future documents by providing notice pursuant to this Agreement.

20. Payment of Permits/Licenses

Contractor bears responsibility to obtain any license, permit, or approval required from any agency for work/services to be performed under this Agreement at Contractor's own expense prior to commencement of said work/services. Failure to do so will result in forfeit of any right to compensation under this Agreement.

21. Prevailing Wage

When applicable, Contractor hereby agrees to pay not less than prevailing rates of wages and be responsible for compliance with all the provisions of the California Labor Code, Article 2-Wages, Chapter 1, Part 7, Division 2, Section 1770 et seq. A copy of the prevailing wage scale established by the Department of Industrial Relations is on file in the office of the Director of Public Works, and available at www.dir.ca.gov/DLSR or by phone at 415-703-4774. California Labor Code Section 1776(a) requires each contractor and subcontractor keep accurate payroll records of trades workers on all public works projects and to submit copies of certified payroll records upon request.

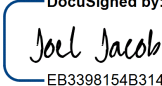
Additionally,

- No contractor or subcontractor may be listed on a bid proposal for a public works project (submitted after March 1, 2015) unless registered with the Department of Industrial Relations pursuant to Labor Code section 1725.5 [with limited exceptions from this requirement for bid purposes only under Labor Code section 1771.1(a)].
- No contractor or subcontractor may be awarded a contract for public work on a public works project (awarded on or after April 1, 2015) unless registered with the Department of Industrial Relations pursuant to Labor Code section 1725.5.
- This project is subject to compliance monitoring and enforcement by the Department of Industrial Relations.

* * *

In witness of and in agreement with this Agreement’s terms, the parties, by their duly authorized representatives, affix their respective signatures:

For Contractor: CDW-G

<div><div>DocuSigned by:</div><div></div><div>EB3398154B31496...</div></div>	12/26/2023 7:57 AM PST	Joel Jacob
Contractor Signature	Date	Contractor Name (please print)

COUNTY OF SAN MATEO

By:
President, Board of Supervisors, San Mateo County

Date:

ATTEST:

By:
Clerk of Said Board

30171, 30115

Budget

EXHIBIT A

PRIVATE PRICING AGREEMENT

This Private Pricing Agreement ("PPA") is entered into by and between the parties listed on this page. PPA

Effective Date: The date the last party signs this PPA.

1. Pricing Terms.

Term	Meaning
Specified End Customer	San Mateo County Sherriff's Office
Discount Term	January 1, 2023-December 31, 2027
Contract Year	Contract Year 1: January 1, 2023-December 31, 2023 Contract Year 2: January 1, 2024-December 31, 2024 Contract Year 3: January 1, 2025-December 31, 2025 Contract Year 4: January 1, 2026 – December 31, 2026 Contract Year 5: January 1, 2027-December 31, 2027
Eligible Payer Accounts	Program Management Accounts with the following AWS account IDs: 2605-8807-4839
Cross-Service Discount	8%
Spend Commitment	Contract Year 1: \$300,000 Contract Year 2: \$300,000 Contract Year 3: \$300,000 Contract Year 4: \$300,000 Contract Year 5: \$300,000
Commitment-Eligible Fees	The following amounts incurred under Eligible Accounts (excluding fees paid for by applying the Available Balance in accordance with Section 6, excluding taxes, and net of any applicable discounts and refunds), which count towards your Spend Commitment: (a) fees for use of Services (other than AWS Professional Services, AWS Training and AWS Certification) in Eligible Regions; (b) except as set forth in (c), fees for purchases on AWS Marketplace that are deployed on the Services (other than purchases of professional services) up to a maximum of 25% of the then-applicable Spend Commitment; and (c) fees for use of Commitment-Eligible Products.
Step-Up Discount Term	The five-year period beginning on the Step-Up Effective Date.
Step-Up Contract Year	Step-Up Contract Year 1: the one-year period beginning on the Step-Up Effective Date Step-Up Contract Year 2: the one-year period beginning on the first anniversary of the Step-Up Effective Date

Term	Meaning
	Step-Up Contract Year 3: the one-year period beginning on the second anniversary of the Step-Up Effective Date
	Step-Up Contract Year 4: the one-year period beginning on the third anniversary of the Step-Up Effective Date
	Step-Up Contract Year 5: the one-year period beginning on the fourth anniversary of the Step-Up Effective Date
Step-Up Cross-Service Discount	8.5%
Step-Up Spend Commitment	Step-Up Contract Year 1: \$500,000 Step-Up Contract Year 2: \$500,000 Step-Up Contract Year 3: \$500,000 Step-Up Contract Year 4: \$500,000 Step-Up Contract Year 5: \$500,000

2. Discount. CDW will apply the Cross-Service Discount to fees for use of Eligible Services. CDW will apply any discounting expressed as a percentage to Public Pricing. The discounting under this PPA may not be combined with any other discounts (including with any discounts on the AWS Site). CDW will apply the Cross-Service Discount except where any component of an Eligible Service is entitled to discounting under another agreement (other than any ordering documents entered into pursuant to this PPA). CDW will apply the discounting under this PPA during the Discount Term so long as you are complying with the terms of this PPA.

3. Commitment. Effective as of the first day of the applicable Contract Year, you agree to incur Commitment-Eligible Fees during each Contract Year at least equal to the corresponding Spend Commitment payment obligation. If the Commitment-Eligible Fees incurred during a Contract Year are less than the corresponding Spend Commitment payment obligation, then you will pay CDW a Spend Commitment Shortfall Payment.

4. Commitment Step-Up. If during the first three years of the Discount Term you submit a Step-Up Notice to aws-notification-intake@amazon.com, then effective as of the Step-Up Effective Date: (i) the Discount Term will be extended until the end of the Step-Up Discount Term; and (ii) references in this PPA to "Cross-Service Discount", "Spend Commitment" and "Contract Year" will be read as references to "Step-Up Cross-Service Discount", "Step-Up Spend Commitment" and "Step-Up Contract Year", respectively. For clarity: (x) you will continue to owe any Spend Commitment Shortfall Payment obligations incurred prior to the Step-Up Effective Date; and (y) CDW will not apply the Step-Up Cross-Service Discount to any fees incurred prior to the Step-Up Effective Date. If you submit a Step-Up Notice to the AWS email box as set forth above, you agree to provide CDW with written notice of your submission.

5. Payments. Except as otherwise provided in this PPA, you will pay all fees for use of Eligible Services and other amounts due under this PPA via check or wire transfer and in accordance with the payment terms of the Agreement. You will make all such payments to CDW in US dollars. All payment obligations

under this PPA will survive expiration or termination of this PPA.

6. Available Balance. During the term of this PPA, COW will apply the Available Balance to fees and any taxes for use of Eligible Services provided by the AWS Party to which the applicable portion of the Available Balance is paid. The Available Balance is nonrefundable, will not reduce your Spend Commitment Shortfall Payment obligations, and is not a deposit for or credit toward the purchase of any services after the Discount Term. After the Discount Term, COW will invoice you for an amount equal to any remaining Available Balance, and the Available Balance will be applied against such invoiced amount.

7. Term; Termination.

a. Term. The term of this PPA commences on the PPA Effective Date and ends on the last day of the Discount Term.

b. Termination. This PPA will automatically terminate upon any termination of any Material Agreement. Notwithstanding any termination for convenience rights in any Agreement, you may only terminate this PPA or any Agreement for convenience during the Discount Term if each of the following is satisfied: (i) you fail to exercise or fund an option, terminate for convenience, or otherwise materially de-scopes requirements associated with the Eligible Accounts (a "Government Termination") under any agreement(s) between you and the Public Sector End Customer involving your resale of Eligible Services (a "Government Contract"); (ii) the Public Sector End Customer continues to utilize the Eligible Services for the scope of work associated with the Government Contract, directly or through a successor contractor; (iii) you notify COW within 20 days following the occurrence of the foregoing events, including documentation substantiating the Government Termination (which notice COW will pass along through the chain of distribution to AWS); (iv) such Government Termination occurs no earlier than one year after the PPA Effective Date; and (v) promptly following the Government Termination, the parties will discuss in good faith the possibility of amending the parties' future obligations under this PPA to reflect a lower Spend Commitment and adjusted Cross Service Discount (however, nothing in this Section obligates either party to enter into any amendment or modification to the terms of this PPA). You will notify COW as soon as practicable upon learning of or reasonably suspecting a forthcoming Government Termination. Any such termination for convenience satisfying these conditions will be effective on the effective date of any Government Termination or the date AWS is provided Notice of the Government Termination, whichever date is later. In the event of a Government Termination where the Public Sector End Customer does not continue to utilize the Eligible Services per Section 7(ii) above, COW will, upon written notice to you, terminate this PPA and you will pay COW an amount equal to the total value of the discounting received under this PPA as of the effective date of termination. Each party may terminate this PPA for cause upon written notice if the other party is in material breach of this PPA, provided that the breaching party will have 30 days from receipt of the notice to cure any material breach that can be cured.

8. Enterprise Support. Unless the Eligible Accounts are already enrolled will, starting on the first day of the Discount Term, enroll the Eligible Accounts in AWS Enterprise Support (either AWS Partner- Led Support or AWS Resold Support). You will maintain any such enrollment throughout the term of this PPA.

9. References. You grant to CDW and its Affiliates (for the benefit of Waste whom COW may sublicense these rights) a non-exclusive, worldwide, royalty-free right and license to use your entity name and logos (provided promptly by you to COW and its Affiliates, upon COW's or its Affiliate's request) to identify you as an Amazon Web Services customer. This license will survive after the term of this PPA, provided you may terminate this license at any time after termination of this PPA by giving CDW and its Affiliates at least 40 days' written notice. Upon termination of this license, COW will request that AWS and its Affiliates

will remove your entity name and logos from the AWS Site, but AWS and its Affiliates may continue to use your entity name and logos in any other items produced before termination of this license.

10. Nondisclosure. Each party agrees that the existence and terms of this PPA are not publicly known and will not be disclosed by that party. All nondisclosure obligations under this PPA will survive expiration or termination of this PPA.

11. Miscellaneous. The failure of a party to enforce any provision of this PPA will not constitute a present or future waiver of such provision nor limit such party's right to enforce such provision at a later time. All waivers by a party must be in writing to be effective. With respect to the subject matter hereof, this PPA, together with the Agreements, each as amended by this PPA: (a) is intended by the parties as the final, complete and exclusive expression of the terms of their agreement; and (b) supersedes all prior agreements and understandings (whether oral or written) between the parties. If there is a conflict between an Agreement and this PPA, this PPA will prevail. If there is a conflict between this PPA and any other amendment or addendum to any Agreement or to this PPA, the document later in time will prevail. Any Spend Commitment and Spend Commitment Shortfall Payment is a payment obligation under the payment terms of the applicable Agreement.

12. Definitions. For purposes of this PPA, capitalized terms have the meanings set forth in an Agreement, or as described on the AWS Site unless otherwise defined in this PPA.

"Affiliate" means any entity that directly or indirectly controls, is controlled by or is under common control with that party.

"Agreement" means any written agreement between CDW and you governing your use of the Services other than this PPA.

"Available Balance" means the remaining balance of any Spend Commitment Shortfall Payment paid to CDW during the term of this PPA.

"AWS" means Amazon Web Services, Inc. ("AWS, Inc.") and each other entity identified at <https://aws.amazon.com/legal/aws-contracting-party> that has agreed, following your request, to become a party to this PPA based on the location you have set for an Eligible Account (each, an "AWS Party").

"AWS Partner-Led Support" means the AWS Support provided by AWS to you.

"Commitment-Eligible Products" means the products and services listed at \ <https://commitment-eligible-products-list.s3.amazonaws.com/Commitment+Eligible+Products+SP.pdf>

"Eligible Accounts" means the following AWS accounts: (i) the Eligible Payer Accounts, other than any Eligible Payer Account that CDW agrees to remove at your request; (ii) any Program Management Account that CDW agrees to add as an Eligible Payer Account at your request; and (iii) any accounts commonly identified by AWS as Member Accounts ("Member Accounts") joined via organizations commonly identified by AWS as "AWS Organizations" ("AWS Organizations") to an Eligible Payer Account; provided that: (x) this PPA applies only to Member Accounts that are for use by the Specified End Customer (provided that such customer purchases Services for its internal use, not for sale to a third party) and that are used by such End Customer during the Discount Term only as accounts commonly identified by AWS as "Program Accounts";

(y) Eligible Payer Accounts cannot be joined via AWS Organizations to any AWS accounts other than such Member Accounts; and (z) this PPA applies only to AWS accounts that are associated with a location that corresponds to an AWS Party.

"Eligible Regions" means the AWS regions and locations available to you and identified on the AWS Site

at https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2 (except Mainland China Regions), as may be updated from time to time.

"Eligible Services" means the Services listed at <https://solutionprovider.s3.amazonaws.com/Solution+Provider+Eligible+Services+List.pdf> used in Eligible Regions under Eligible Accounts.

"Public Pricing" means the pricing for the Eligible Services as described on the AWS Site.

"Public Sector End Customer" means the County of San Mateo.

"Spend Commitment Shortfall Payment" means an amount equal to the Spend Commitment for the applicable Contract Year less the Commitment-Eligible Fees incurred during such Contract Year.

"Step-Up Effective Date" means the first day of the month after AWS receives the Step-Up Notice, provided such Step-Up Notice is received by the 20th of the month; otherwise, the first day of the second month after receipt of the Step-Up Notice.

"Step-Up Notice" means a completed and signed notice in the form attached as Attachment 1.

EXHIBIT B

AWS CLOUD SERVICES ADDENDUM FOR SOLUTION PROVIDER ACCOUNTS

This AWS Cloud Services Addendum for Solution Provider Accounts for Public Sector Customers ("Addendum") forms part of the Statement of Work between Customer and CDW and cannot be modified.

1. AWS-ENABLED SOLUTIONS

- 1.1. CDW and its affiliates have a reseller relationship with Amazon Web Services, Inc. and its affiliates ("AWS"). As part of such arrangement, CDW is authorized to make certain AWS services available to Customer as part of the products and services that CDW is delivering to Customer under the SOW (collectively, "AWS-Enabled Solutions"). If required by the Agreement or SOW, Customer hereby approves of CDW's use of AWS as an authorized subcontractor.
- 1.2. CDW is reselling AWS services under this Addendum through the AWS Solution Provider Program. CDW will designate Customer accounts as "Solution Provider Accounts." By entering into this Addendum, Customer acknowledges that Customer's use of the AWS services portion of the AWS- Enabled Solutions is governed by this Addendum, the SOW and the Agreement, and not by the terms of an agreement with AWS. Customer further acknowledges that CDW is not making any representations, warranties, or guarantees with respect to the AWS services on AWS's behalf, and that CDW is not holding itself out as an agent of AWS.
- 1.3. Customer will not, and will ensure its End Users (defined below) do not, bring a claim against AWS, its affiliates or any of their respective employees, officers, directors, and representatives where such claim arises from or relates to the Solution Provider Accounts, except where the relevant claim arises solely out of the gross negligence, willful misconduct, or violation of applicable law by AWS in its delivery of the AWS services and the losses arising out of such claim could not have been prevented by Customer or its End Users via their use, delivery, or management of such Solution Provider Accounts, such as via encryption, account monitoring, account access management, backup and redundancy, etc. Customer's breach of this paragraph will not be subject to any exclusion or limitation of liability under the Agreement or this Addendum.
- 1.4. This Addendum incorporates by reference the latest version of the AWS Public Sector Access Policy, a current version of which is located at <https://s3.amazonaws.com/Reseller-Program-Legal-Documents/AWS+Access+Policy.pdf> (as it may be updated by AWS from time to time, and as may be available on any successor or related site designated by AWS).

2. LIMITATIONS ON USE OF AWS-ENABLED SOLUTIONS

- 2.1. This Addendum authorizes Customer's use of AWS-Enabled Solutions only where Customer is the end user of the AWS-Enabled Solutions. Customer may not re-distribute the AWS-Enabled Solutions. Customer represents and warrants that Customer is buying the AWS-Enabled Solutions for Customer's own internal use and not for resale.
- 2.2. This Addendum authorizes Customer's use of AWS-Enabled Solutions only where Customer is a Public Sector Customer not located in the AWS Exclusive Area. "Public Sector Customer" means a Customer that is an agency, organization, or other entity that is within (or is substantially owned, funded, managed or controlled by): (i) the executive, legislative, or judicial branches of any government within the U.S. (federal, state or local) and its territories; or by any other country's government at any level; (ii) a quasi-governmental entity (such as the World Bank); (iii) an international governing/regulatory body (such as

an EU institution); (iv) a publicly funded institution (such as a college, university, or hospitals); or (v) a higher-tier prime contractor, consultant, or other entity working in support of the foregoing. "AWS Exclusive Area" means the area within the European Economic Area that AWS has reserved for its own sale of AWS services, described at <https://s3-us-west-2.amazonaws.com/solution-provider-program-legal-documents/AWS+Exclusive+Area.pdf>, as it may be updated by AWS from time to time, and as may be available on any successor or related site designated by AWS.

3. AWS GOV CLOUD TERMS. The provisions of this Section 3 apply to Customer's use of AWS-Enabled Solutions for the AWS GovCloud (US) Region ("GovCloud Region").

- 3.1. Customer represents and warrants that it (i) is a U.S. Person, as defined by 22 CFR part 120.15 ("U.S. Person"); (ii) will only assign a U.S. Person as its account owner for the GovCloud Region; (iii) if required by the International Traffic In Arms Regulations ("ITAR"), it has and will maintain a valid Directorate of Defense Trade Controls registration; (iv) is not subject to export restrictions under U.S. export control laws and regulations (e.g., Customer is not a denied or debarred party or otherwise subject to sanctions); and (v) maintains an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including the ITAR. If requested, Customer agrees to provide additional documentation and cooperation to verify the accuracy of the foregoing representations and warranties.
- 3.2. Customer is responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, Customer account access, data transmission, encryption, and appropriate storage and processing of data within the GovCloud Region. Customer is responsible for verifying that all End Users accessing Customer Materials in the GovCloud Region are eligible to gain access to those materials. The AWS-Enabled Solutions may not be used to process or store classified data. If Customer introduces classified data into the AWS Network, Customer will be responsible for all sanitization costs incurred by AWS. Customer's liability under this provision is exempt from any limitations of liability.
- 3.3. Accessing the GovCloud Region requires specific credentials for that region ("GovCloud Credentials"). GovCloud Credentials may be provided to Customers in one of the following ways: (a) CDW may obtain GovCloud Credentials from AWS and transfer them to Customer, and (b) Customer may obtain GovCloud Credentials directly from AWS if Customer has root level access to the relevant Customer account. Customer may initiate this process by contacting AWS at aws-govcloud-us@amazon.com.
- 3.4. Customer represents, warrants, and covenants as follows.
 - 3.4.1. Services may not be used to process or store classified data. If Customer introduces classified data into the AWS Network, Customer will be responsible for all sanitization costs incurred by AWS. Customer's liability with respect to sanitization costs under this provision is exempt from any limitations of liability. "AWS Network" means AWS's data center facilities, servers, networking equipment, storage media, and host software systems (e.g., virtual firewalls) used by AWS to provide the Services.
 - 3.4.2. Customer is responsible for verifying that all End Users accessing Customer Content in the GovCloud Region are eligible to gain access to Customer Content. "End User" means any individual or entity that directly or indirectly through another user (a) accesses or uses Customer Content, or (b) otherwise accesses or uses the Services. "Customer Content" means any software (including machine images), data, text, audio, video, or image that Customer or any End User transfers to AWS or CDW for processing, storage or hosting by the Services and any computational results that Customer or any End User derives from the foregoing through their use of the Services.
 - 3.4.3. Customer: (i) is a U.S. Person, as defined by 22 CFR part 120.15 ("U.S. Person"); (ii) will only assign a U.S. Person as its account owner for the GovCloud Region; (iii) if required by the International Traffic In Arms Regulations ("ITAR"), has and will maintain a valid Directorate of Defense Trade Controls registration; (iv) is not subject to export restrictions under U.S. export control laws and regulations (e.g., Customer is not a denied or debarred party or otherwise subject to sanctions);

and

(v) will maintain an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including the ITAR.

- 3.5. If requested, Customer will provide additional documentation and cooperation to verify the accuracy of the foregoing representations, warranties, and covenants of Section 2 above.
- 3.6. CDW will ensure that AWS abides by the information security program that AWS maintains for the GovCloud Region, as may be updated by AWS from time to time. Such program will supersede any other information security program applicable to the Services under this SOW for the GovCloud Region.
- 3.7. Except to the extent such controls are the subject of Services provided by CDW, Customer is responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, Customer's account access, data transmission, encryption, and appropriate storage and processing of data within the GovCloud Region.

4. USE OF AWS-ENABLED SOLUTIONS

- 4.1. Customer may access and use the AWS-Enabled Solutions in accordance with this Addendum, the SOW and Agreement. Customer will adhere to all laws, rules, and regulations applicable to Customer's use of the AWS-Enabled Solutions. In addition, in its use of the AWS services, Customer will adhere to the AWS Policies. "AWS Policies" means (a) the policy currently available at <http://aws.amazon.com/aup> ("Acceptable Use Policy"), (b) the terms of use located at <http://aws.amazon.com/terms> ("Site Terms"), (c) the rights and restrictions for AWS services located at <http://aws.amazon.com/serviceterms> ("Service Terms"), (d) the privacy policy located at <http://aws.amazon.com/privacy> ("Privacy Policy"), (e) the guidelines and trademark license located at <http://aws.amazon.com/trademark-guidelines> ("Trademark Use Guidelines"), (f) the restrictions described in the software (including machine images), data, text, audio, video, images or other content ("Materials") made available by AWS in connection with AWS services (but excluding the AWS services and Third Party Materials (defined below)), including APIs; WSDLs; sample code; software libraries; command line tools; proofs of concept; templates; and other related technology (including any of the foregoing that are provided by AWS personnel); and further including the following items of documentation: developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals and specifications for AWS services located at <http://aws.amazon.com/documentation> ("Documentation"), and (g) restrictions described at or at <http://aws.amazon.com> and any successor or related site ("AWSite").
- 4.2. As between Customer and CDW, CDW and its suppliers (including AWS) own and reserve all right, title, and interest in and to the AWS-Enabled Solutions. Except as provided in this Addendum, Customer obtains no rights to the AWS-Enabled Solutions, including any related intellectual property rights. Some Materials may be provided to Customer under a separate license, such as the Apache Software License, located at <http://apache.org/licenses/>, or other open source license. In the event of a conflict between this Addendum and any separate license, the separate license will prevail with respect to those Materials.
- 4.3. Customer may not use the AWS-Enabled Solutions in any manner or for any purpose other than as expressly permitted by this Addendum. Customer may not, and may not attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the AWS-Enabled Solutions (except to the extent software included in the AWS-Enabled Solutions is provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the AWS-Enabled Solutions or apply any other process or procedure to derive the source code of any software included in the AWS-Enabled Solutions, (c) access or use the AWS-Enabled Solutions in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (d) resell or sublicense the AWS-Enabled Solutions.
- 4.4. CDW may provide Customer with access to Solution Provider Accounts through AWS Identity and Access

Management functionality or by providing root user credentials. If CDW provides Customer with root user credentials, Customer is responsible for all activities that occur under the Solution Provider Accounts. Customer will not sell, transfer, or sublicense root credentials to any other party, except any agents or subcontractors performing work on its behalf. Customer agrees to notify CDW promptly of any unauthorized use of Solution Provider Accounts, including any root credentials, or any other suspected breach of security relating to the Solution Provider Accounts.

- 4.5. If CDW or AWS makes available to Customer any third party Materials on the AWS Site or in conjunction with the AWS services ("Third Party Materials"), such as software applications provided by third parties, such materials are made available directly to Customer by other companies or individuals under separate terms and conditions, including separate fees and charges. Customer's use of any such Third Party Materials is at Customer's sole risk.
- 4.6. Except as provided in a SOW, Customer is solely responsible for the development, content, operation, maintenance, and use of Customer Materials. For example, Customer is solely responsible for: (a) the technical operation of Customer Materials, including ensuring that calls Customer makes to any AWS service are compatible with then-current APIs for that service; (b) compliance of Customer Materials with the Acceptable Use Policy, the other AWS Policies, and applicable law; (c) any claims relating to Customer Materials; (d) properly handling and processing notices sent to Customer (or any of Customer's affiliates) by any person claiming that Customer Materials violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act; and (e) obtaining all necessary consents to allow CDW and AWS to collect, process, and use any personal data transferred to CDW or AWS by Customer or an End User in connection with Customer's or any End User's use of the AWS-Enabled Solutions. Customer represents and warrants to CDW that Customer or Customer's licensors own all right, title, and interest in and to Customer Materials. "Customer Materials" means Materials Customer transfers to CDW or AWS for processing, storage or hosting by the AWS-Enabled Solutions and any computational results that Customer derives from the foregoing through Customer's use of the AWS-Enabled Solutions. For example, Customer Materials includes Materials that Customer or any End User stores in Amazon Simple Storage Service. Customer Materials does not include Account Information. "Account Information" means information that is provided to AWS in connection with the creation or administration of the AWS account. For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with the AWS account.
- 4.7. Customer is responsible for properly configuring and using the AWS-Enabled Solutions and taking its own steps to maintain appropriate security, protection and backup of Customer Materials, which may include the use of encryption technology to protect Customer Materials from unauthorized access and routinely archiving Customer Materials.
- 4.8. Customer is deemed to have taken any action that Customer permits, assists or facilitates any person or entity to take, including its End Users, related to the AWS-Enabled Solutions. "End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Customer Materials; or (b) otherwise accesses or uses the AWS-Enabled Solutions through Customer. Customer is responsible for End Users' use of Customer Materials and the AWS-Enabled Solutions. Customer will ensure that all End Users comply with Customer's obligations under this Addendum and that the terms of Customer's agreement with each End User are consistent with this Addendum. If Customer becomes aware of any violation of its obligations under this Addendum by an End User, Customer will immediately terminate such End User's access to Customer Materials and the AWS-Enabled Solutions.
- 4.9. In connection with this Addendum, Customer will comply with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations, including all such laws and regulations that apply to a U.S. company, such as the Export Administration Regulations, the International Traffic in Arms Regulations, and economic sanctions programs implemented by the Office of Foreign Assets Control. For clarity, Customer is solely responsible for compliance related to the manner in which Customer chooses to access and use, including Customer's transfer and processing of Customer Materials, the provision of Customer

Materials to End Users, and the AWS region in which any of the foregoing occur. Customer represents and warrants that Customer and Customer's financial institutions, or any party that owns or controls Customer or Customer's financial institutions, are not subject to sanctions or otherwise designated on any list of prohibited or restricted parties, including but not limited to the lists maintained by the United Nations Security Council, the U.S. Government (e.g., the Specially Designated Nationals List and Foreign Sanctions Evaders List of the U.S. Department of Treasury, and the Entity List of the U.S. Department of Commerce), the European Union or its member states, or other applicable government authority.

- 4.10. Customer will comply with all applicable laws, regulations, and contractual requirements (including, but not limited to, applicable Data Protection Laws, Customer Content Requirements, and Public Records Laws) (collectively, "Public Sector Rules") in connection the AWS-Enabled Solutions. Customer will not use the AWS-Enabled Solutions where doing so would result in a breach of Public Sector Rules for either AWS or CDW (each being a "Public Sector Liability"). "Data Protection Laws" means any laws, regulations, or similar legal obligations regarding security, safety, privacy, or similar qualitative or quantitative standards relating to information or data (including, but not limited to, the processing, storage, use of, access to, or transmission of such data) that may apply to the AWS services. "Customer Content Requirements" means any requirements applicable to Customer or agreed upon between CDW and Customer regarding the treatment or management of Customer Materials (e.g., security, location, storage, durability, reliability, redundancy, etc.) in connection with the AWS-Enabled Solutions. "Public Records Laws" means any law, regulation, or official policy relating to an entity's obligation to maintain, preserve, and/or disclose content, documentation, or other records maintained by or on behalf of Customer (including, but not limited to, "Freedom of Information," "Public Records," "Open Records," or "Archives" laws, or other similar requirements at any level of government).

5. SERVICE LEVELS AND SUPPORT

- 5.1. AWS makes certain service level commitments to CDW in its agreement with CDW. CDW is eligible for remedies under a service level agreement only as determined by AWS. If AWS issues a credit to CDW under a service level agreement and Customer would be entitled to a service level credit under this Addendum, AWS will issue the credit to CDW and CDW will pass through the credit to Customer, as applicable. Customer acknowledges that AWS may change the service level commitments from time to time.
- 5.2. CDW will provide support for the AWS-Enabled Solutions as described in the SOW. If CDW provides support directly to Customer (instead of reselling AWS support to Customer), Customer will not open support cases directly with AWS.

6. AWS'S RIGHTS

- 6.1. Customer acknowledges that AWS may do any of the following, which will change, modify or otherwise affect the scope of the AWS services provided by CDW under this Addendum. CDW will have no liability to Customer for any such actions taken by AWS. CDW will use commercially reasonable efforts to notify Customer in advance if CDW knows any such actions are to be taken by AWS.
 - 6.1.1. AWS may remove a territory (e.g., state, country or region) from which the AWS-Enabled Solutions may be offered. Any such removal of a territory will remove such territory from the scope of this Addendum, as applicable.
 - 6.1.2. AWS may suspend or terminate CDW's right to sell the AWS-Enabled Solutions, CDW's right to sell the AWS-Enabled Solutions under a specific resale model, or CDW's right to access or use the AWS services. Any such suspension or termination will suspend the provision of or remove such AWS-Enabled Solutions from the scope of this Addendum, as applicable.
 - 6.1.3. AWS may terminate CDW-provided support or AWS support resold support at anytime.

- 6.1.4. AWS may remove or disable access to content that violates the Acceptable Use Policy, and may require CDW's assistance in doing so.
- 6.1.5. AWS may change or discontinue any of the AWS services, any APIs for the AWS services, or change or remove functionality of any or all of the AWS services from time to time.
- 6.1.6. AWS may add new features or functionality to, or remove existing features or functionality from, its products.
- 6.1.7. AWS may send direct communications to Customer related to the terms of its agreement or the operation or delivery of the AWS-Enabled Solutions.
- 6.1.8. AWS may process usage data related to AWS services accounts, such as resource identifiers, metadata tags, security and access roles, rules, usage policies, permissions, usage statistics and analytics, both in the service regions selected and in the United States.
- 6.1.9. AWS may change the terms of Public Sector Access Policy at any time.
- 6.2. If CDW's performance of any of its obligations relating to the AWS-Enabled Solutions is prevented, hindered or delayed due to acts or omissions of AWS, then CDW's non-performance will be excused, provided that CDW uses commercially reasonable efforts to recommence performance whenever and to whatever extent possible without delay, including through the use of alternate sources, workaround plans, or other means.
- 6.3. Customer will remain liable to CDW if AWS terminates or suspends Customer's AWS-Enabled Solutions due to the acts or omissions of Customer.

7. CUSTOMER OBLIGATIONS

- 7.1. Customer will cooperate in good faith with CDW in CDW's investigation into any complaints concerning the AWS services and, in any audit, requested by AWS.
- 7.2. If Customer provides any Suggestions to CDW or AWS, AWS will own all right, title, and interest in and to the Suggestions, even if Customer has designated the Suggestions as confidential. AWS will be entitled to use the Suggestions without restriction. Customer hereby irrevocably assigns to AWS all right, title, and interest in and to the Suggestions and agrees to provide AWS any assistance AWS may require to document, perfect, and maintain AWS's rights in the Suggestions. "Suggestions" means all suggested improvements to the AWS services, the AWS Site or AWS Materials that Customer provides to AWS or CDW.
- 7.3. Customer will supply CDW with a current and accurate legal name, telephone number, email address, city, state/region, country and zip/postal code, and other information as may be required from time to time by AWS. Customer acknowledges that AWS may use this information in connection with misuse or suspected misuse of the AWS services by Customer, to monitor Customer's account, and to effect any transition of Customer's AWS services. AWS may further disclose this and other information associated with Customer's use of the AWS services to third parties who provide solutions to Customer as part of the AWS-Enabled Solutions.
- 7.4. Customer will maintain up-to-date notice addresses in order to receive notices from CDW regarding the AWS services that may affect Customer.
- 7.5. Customer acknowledges that AWS may capture, retain and use network or usage information relating to Customer's access or use of the AWS services.

8. FEES AND TAXES

- 8.1. Customer will pay for the AWS-Enabled Solutions as described in the Agreement and SOW, except that if any taxes (for example, international withholding taxes) are required to be withheld on any payment by Customer, Customer will pay such additional amounts as are necessary so that the net amount received by CDW is equal to the amount then due and payable. CDW will provide Customer with such tax forms as are reasonably requested to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made for the AWS-Enabled Solutions.

9. DATA PRIVACY AND SECURITY

- 9.1. The sections of the Agreement and SOW (to the extent applicable) governing the privacy and security of Customer's data will not apply to the AWS services and Customer Materials and will be superseded in their entirety by the terms and conditions set forth in this Section 9.
- 9.2. CDW will ensure that AWS implements reasonable and appropriate measures for the AWS data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within AWS's control and are used to provide the AWS services (the "AWS Network") designed to help Customer (i) secure Customer Materials against accidental or unlawful loss, access or disclosure, and (ii) with respect to the use of the GovCloud Region only, (1) implement the in-scope Federal Risk and Authorization Management Program ("FedRamp") controls for the AWS services identified as FedRamp Compliant, and (2) maintain physical and logical access controls to limit access to the AWS Network by AWS personnel, including employees and contractors, to U.S. Citizens, as defined by 8 USC §1401, et seq ("U.S. Citizens") (collectively, the "Security Objectives"), in accordance with the AWS Security Standards set forth on Exhibit A.
- 9.3. CDW will ensure that AWS implements reasonable measures designed to maintain the integrity of the AWS Network against: (a) unauthorized or unlawful processing of personal data (as these terms are defined in applicable data legislation); and (b) accidental or unauthorized destruction of, damage to, alteration of, or disclosure of personal data. To the extent personal data is included in Customer Materials, CDW will ensure that AWS will only process such personal data as necessary to provide the AWS services.
- 9.4. Notwithstanding the foregoing, CDW will ensure that AWS maintains an information security program designed to provide at least the same level of protection as evidenced by the certification standards (e.g. ISO 27001, ISO 27018, ISO 27017, ISO 9001, PCI DSS) AWS agrees to from time to time.
- 9.5. In lieu of any other rights Customer may have with respect to an audit of the AWS services, Customer will be entitled to the rights described in this paragraph. To the extent AWS provides CDW with access to AWS's third party security audits annually (e.g., SOC 1 Type 2/ SOC 2 Type 2 reports), then upon request by Customer, CDW will use commercially reasonable efforts to obtain AWS's permission for these audits to be shared with Customer. For the avoidance of doubt, it will not constitute a breach of CDW's obligations pursuant to this Section 9 if exceptions are identified in any SOC 1 Report or SOC 2 Report (or, in either case, its equivalent).
- 9.6. Customer may specify the AWS regions in which Customer Materials will be stored. Customer consents to the storage of Customer Materials in, and transfer of Customer Materials into, the AWS regions Customer selects. CDW will not (a) disclose Customer Materials to any government or third party, or (b) subject to Section 6.1.8, move Customer Materials from the AWS regions selected by Customer, except in each case as necessary to comply with the law or a binding order of a governmental body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, CDW will give Customer reasonable notice of any legal requirement or order referred to in this Section to allow Customer to seek a protective order or other appropriate remedy.

- 9.7. If CDW has actual knowledge of the unauthorized access to or acquisition of any record containing Customer Materials that is subject to applicable data breach notification law and such access or acquisition is caused by a confirmed breach of the AWS Security Standards that renders misuse of the information reasonably likely, CDW will
- (a) promptly notify Customer, as required by applicable law, and (b) take commercially reasonable measures to address the breach in a timely manner.
- 9.8. Customer hereby consents to allow AWS to collect, process, and use any personal data of Customer that is transferred to AWS for purposes of (a) providing the AWS-Enabled Solutions, (b) the business relationship between AWS and CDW, or (c) marketing and providing AWS services to Customer and CDW.

10. WARRANTIES AND INDEMNITIES

- 10.1. Each party represents and warrants to the other that: (a) it will comply with all applicable laws, rules, regulations and ordinances in the performance of this Addendum, including but not limited to import, re-import, export and re-export control laws and regulations, including the Export Administration Regulations, the International Traffic in Arms Regulations and country-specific economic sanctions programs implemented by the Office of Foreign Assets Control;
- (b) its performance hereunder does not breach any other agreement to which it is bound; (c) it has the full power and authority to enter in and perform this Addendum; and (d) the execution and delivery of this Addendum has been duly authorized. Notwithstanding the foregoing set forth in subpart (a) above, Customer is solely responsible for compliance with applicable laws related to the manner in which Customer chooses to use the AWS services, including
- (i) any transfer and processing of Customer Materials; (ii) the provision of Customer Materials to third parties and
- (iii) specifying the AWS region in which any of the foregoing occur.
- 10.2. CDW represents and warrants to Customer that: (a) the AWS services portion of the AWS-Enabled Solutions will perform substantially in accordance with the Documentation, and (b) it will use commercially reasonable efforts to ensure that those portions of the AWS services that are of a type ordinarily affected by viruses utilize enterprise-grade security software designed to detect and remove malicious or hidden mechanisms or code designed to damage or corrupt the AWS services or Customer Materials. For any breach of this Section, as Customer's sole and exclusive remedy, CDW will provide the remedies made available by AWS in connection with such breach as applicable to Customer.
- 10.3. Customer will defend, indemnify, and hold harmless CDW, its affiliates and licensors (including AWS), and each of their respective employees, officers, directors, and representatives from and against any claims, damages, losses, liabilities, costs and expenses (including reasonable attorneys' fees) arising out of or relating to any third party claim concerning (a) Customer or any End User's use of the AWS services in a manner not authorized by this Addendum (including any activities under the AWS account and use by Customer's employees and personnel); (b) any breach of this Addendum or violation of applicable law, including breaching Public Sector Rules, by Customer or any End User;
- (c) alleged infringement or misappropriation of any third party rights by Customer Materials, or by the use, development, design, production, advertising or marketing of Customer Materials; or (d) a dispute between Customer and any of its End Users. The foregoing indemnification obligation will not be subject to any limitation of liability contained in the SOW, Agreement, or elsewhere, and will survive termination or expiration of the SOW and Agreement. The indemnified parties are third party beneficiaries of the indemnifying party's obligations under this paragraph.
- 10.4. If a third party asserts a claim against Customer or its employees, officers, and directors alleging that the AWS services portion of the AWS-Enabled Solutions infringe or misappropriate that third party's intellectual property rights, CDW will enforce its indemnities on behalf of Customer to the extent CDW is permitted to do so under the terms its agreement with AWS. The remedies provided in this paragraph are the sole

and exclusive remedies for any third party claims of infringement or misappropriation of intellectual property rights by the AWS services portion of the AWS- Enabled Solutions.

- 10.5. CDW ACCEPTS NO LIABILITY FOR ANY CLAIMS ARISING OUT OF ANY ACT OR OMISSION, INCLUDING NEGLIGENCE, BY AWS. EXCEPT AS EXPRESSLY PROVIDED IN THIS ADDENDUM, CDW DOES NOT MAKE OR GIVE ANY REPRESENTATION, CONDITION, SERVICE LEVEL, INDEMNITY OR WARRANTY ABOUT THE AWS SERVICES PORTION OF THE AWS- ENABLED SOLUTIONS, AND THE AWS SERVICES PORTION OF THE AWS-ENABLED SOLUTIONS ARE PROVIDED "AS IS." EXCEPT TO THE EXTENT PROHIBITED BY LAW, CDW, ITS AFFILIATES AND ITS LICENSORS MAKE NO OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING THE AWS SERVICES PORTION OF THE AWS-ENABLED SOLUTIONS OR THIRD PARTY MATERIALS, AND DISCLAIM ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (A) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (B) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (C) THAT THE AWS SERVICES PORTION OF THE AWS-ENABLED SOLUTIONS OR THIRD PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (D) THAT ANY MATERIALS, INCLUDING CUSTOMER MATERIALS OR DATA, OR THIRD PARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. AWS-ENABLED SOLUTIONS ARE NOT DESIGNED FOR USE IN LIFE SUPPORT, LIFE SUSTAINING, NUCLEAR SYSTEMS OR OTHER APPLICATIONS IN WHICH FAILURE OF SUCH AWS- ENABLED SOLUTIONS COULD REASONABLY BE EXPECTED TO RESULT IN PERSONAL INJURY, LOSS OF LIFE OR PROPERTY DAMAGE. USE IN ANY SUCH APPLICATIONS IS AT CUSTOMER'S SOLERISK.

11. SUSPENSION

- 11.1. CDW may suspend Customer's or any End User's right to access or use any portion of the AWS-Enabled Solutions immediately if CDW determines: Customer is, or any End User is, in breach of its payment obligations or any other obligation of this Addendum; or Customer's or an End User's use of the AWS Enabled-Solutions (i) poses a security risk to the AWS Enabled-Solutions or any other third party, (ii) may adversely impact the AWS Enabled-Solutions or the systems or Materials of any other CDW or AWS customer, (iii) may subject CDW, AWS or any third party to liability, or (iv) may be fraudulent.
- 11.2. If CDW suspends Customer's right to access or use any portion of the AWS Enabled-Solutions:
- 11.2.1. Customer remains responsible for all fees and charges Customer incurs during the period of suspension;
 - 11.2.2. Customer will not be entitled to any service credits under any service level agreement between CDW and AWS, if applicable; and
 - 11.2.3. If requested by Customer, Customer will be permitted to retrieve Customer Materials from the AWS- Enabled Solutions that are subject to suspension, but only to the extent such retrieval is commercially reasonable and technically feasible following suspension, and would not result in or exacerbate any of the conditions giving rise to the suspension.

12. TERM; TERMINATION; EFFECT OF TERMINATION

- 12.1. The term of this Addendum will commence on the Addendum Effective Date and will continue until the earlier of (a) termination of the SOW or (b) a termination of this Addendum as set forth in this Section 12.
- 12.2. CDW may terminate this Addendum if (a) there is an act or omission by Customer or any End User for which CDW has a right to suspend, or (b) upon thirty (30) days' notice to Customer in order to comply with applicable law or requirements of governmental entities.

- 12.3. Either party may terminate this Addendum for cause if the other party is in material breach of this Addendum and the material breach remains uncured for a period of thirty (30) days from receipt of notice by the other party. Upon the termination date:
 - 12.3.1. All of Customer's rights under this Addendum will immediately terminate; and
 - 12.3.2. Customer remains responsible for all fees and charges Customer has incurred for the AWS-Enabled Solutions incurred through the effective date of termination.
- 12.4. During the ninety (90) days following the effective date of termination, Customer may retrieve any of Customer Materials from the AWS-Enabled Solutions unless (i) prohibited by law or the order of a governmental or regulatory body or if permitting retrieval could subject CDW, AWS or a third party to liability, or (ii) Customer has not paid all amounts due for the AWS-Enabled Solutions under this Addendum other than any amounts disputed in good faith.

13. LIMITATION OF LIABILITY

- 13.1. NEITHER PARTY NOR ANY OF THEIR AFFILIATES OR LICENSORS WILL BE LIABLE TO THE OTHER PARTY UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR ANY (A) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, (B) THE VALUE OF LOST DATA, LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, OR GOODWILL, (C) INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY CUSTOMER RELATED TO THIS ADDENDUM, OR (D) UNAVAILABILITY OF ANY OR ALL OF THE AWS SERVICES PORTION OF THE AWS-ENABLED SOLUTIONS (THIS DOES NOT LIMIT ANY SERVICE CREDITS THAT MAY BE AVAILABLE UNDER THIS ADDENDUM).
- 13.2. THE AGGREGATE LIABILITY UNDER THIS ADDENDUM OF CDW AND ANY OF ITS AFFILIATES OR LICENSORS WILL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER TO CDW ATTRIBUTABLE TO THE AWS SERVICES PORTION OF THE AWS-ENABLED SOLUTIONS THAT GAVE RISE TO THE LIABILITY DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE.
- 13.3. The limitations set forth in Section 13.1 and 13.2 do not apply to (a) indemnification obligations, (b) payment obligations, (c) damages for gross negligence or willful misconduct, or (d) breaches of confidentiality (excluding breaches related to Customer Materials).

14. MISCELLANEOUS

- 14.1. Capitalized terms used but not defined in this Addendum will have the meanings ascribed to them in the Agreement or SOW. In the event of a conflict between this Addendum and the SOW or Agreement, this Addendum will control. References in this Addendum to a particular website will be deemed to mean the most current version of that website or a successor website, or any related locations designated by CDW or AWS, all of which are subject to change without notice. Any terms of this Addendum that expressly survive termination or expiration, or by their nature ought to survive termination or expiration, will survive.

Exhibit B - Attachment 1

AWS PUBLIC SECTOR ACCESS POLICY

(Last Updated April 2, 2018)

This AWS Public Sector Access Policy (“**Access Policy**”) is hereby made a part of the agreement (the “**Agreement**”) between [INSERT END CUSTOMER NAME] (“**Customer**”) and [INSERT SOLUTION PROVIDER NAME] (“**Solution Provider**”) regarding Customer’s use of and access to the AWS Services via the AWS accounts provided to Customer by Provider (“**Solution Provider Accounts**”). Section 7 contains definitions of capitalized terms.

1. Scope. This Access Policy is not an agreement with Amazon Web Services, Inc. (“**AWS**”). It sets out the rules, conditions, and restrictions that apply to Customer’s use of the AWS Services under Solution Provider Accounts where (1) Customer does not have an AWS Services Agreement with AWS; or (2) if Customer does have an AWS Services Agreement with AWS, Solution Provider has not designated it to AWS as Customer’s own account under the AWS Solution Provider Program.

2. Use of the Services.

2.1 Generally. Solution Provider gives Customer access to the AWS Services via Solution Provider Accounts, and Customer’s use of and access to the AWS Services is governed by the Agreement and this Access Policy. Contractual commitments by AWS to Solution Provider (for example, service level agreements) do not apply as between Customer and AWS. Customer must look solely to Solution Provider under this Agreement regarding any claims or damages relating to, or arising out of, the AWS Services. Solution Provider is not an agent of AWS and is not acting on behalf of AWS, and Customer is not a third party beneficiary of any agreement between Solution Provider and AWS.

2.2 Disclaimers; Limitations on AWS Liability. THE AWS SERVICES, AWS CONTENT, AND THIRD-PARTY CONTENT ARE PROVIDED “AS IS.” EXCEPT TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, NEITHER AWS, NOR SOLUTION PROVIDER ON BEHALF OF AWS, MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT. AWS DISCLAIMS ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (a) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (b) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (c) THAT THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (d) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST, ALTERED, OR DAMAGED. AWS WILL NOT BE LIABLE TO CUSTOMER FOR ANY DAMAGES OF ANY KIND (INCLUDING DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, DAMAGES FOR LOST PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA, THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY CUSTOMER IN CONNECTION WITH CUSTOMER’S USE OF THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT) ARISING IN CONNECTION WITH, OR RELATED TO, CUSTOMER’S INABILITY TO USE THE AWS SERVICES, INCLUDING AS A RESULT OF ANY TERMINATION OR SUSPENSION OF SOLUTION PROVIDER ACCOUNTS UNDER ANY AGREEMENT BETWEEN AWS AND SOLUTION PROVIDER, DISCONTINUATION OR DOWNTIME OF AWS SERVICES, OR ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ACCOUNT CONTENT.

2.3 Account Keys. Solution Provider may provide Customer with AWS account keys which will allow Customer to directly access the AWS Services via Solution Provider Accounts. AWS is not responsible to Customer for any activities that occur under these account keys, regardless of whether the activities are undertaken by Customer, Solution Provider, or a third party (including Customer employees, contractors or agents) and AWS is not responsible to Customer for unauthorized access to Solution Provider Accounts.

2.4 Third-Party Content. Through the use of the AWS Services or the AWS Site, Customer may have access to Third-Party Content, which is made available directly to Customer by other entities or individuals under separate terms and conditions, including separate fees and charges. Customer’s use of any Third-Party Content is at its sole risk.

2.5 AWS Services Policies. All access to and use of AWS Services is subject to the AWS Services Policies. (Notwithstanding anything in the Acceptable Use Policy and AWS Service Terms, these two AWS Services Policies are not separate agreements between Customer and AWS.)

2.6 Customer Responsibilities. Unless otherwise agreed by Solution Provider, Customer is solely responsible for the development, content, operation, maintenance, and use of Account Content in Solution Provider Accounts, including (a) the technical operation of AWS Services in connection with Account Content; (b) compliance of Account Content with the AWS Services Policies and applicable law; (c) any action Customer permits, assists, or facilitates any other person or entity to take under Solution Provider Accounts; and (d) use of AWS Services or Account Content by End Users under Solution Provider Accounts (and ensuring that End Users comply with Customer obligations under this Access Policy). If Customer becomes aware of any violation of its obligations under this Access Policy caused by itself or an End User, Customer will immediately terminate such End User's access to Account Content and the AWS Services by such End User. Unless otherwise agreed by Solution Provider, Customer is solely responsible for properly configuring and using the AWS Services and otherwise taking appropriate action to secure, protect, and backup Solution Provider Accounts and Account Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Account Content from unauthorized access and routinely archiving Account Content.

3. AWS Services Interruption. AWS may suspend the Solution Provider Accounts used by Customer to access the AWS Services immediately if AWS determines Customer's or an End User's use of the AWS Services (i) violates the AWS Services Policies; (ii) poses a security risk to the AWS Services or any other AWS customer, (iii) may harm AWS systems or the systems or Content of any other AWS customer; or (iv) may subject AWS to liability as a result of any of the foregoing. We will provide notice of any suspension to Solution Provider, who is solely responsible for providing any notices to Customer under the Agreement. Nothing in this Section 3 will operate to limit Customer's rights or remedies otherwise available to Customer against Solution Provider under the Agreement or applicable law.

4. Transition of Solution Provider Accounts. Except as otherwise provided by law or the Agreement, a transition of Solution Provider Accounts from Solution Provider to a third party (or directly to AWS) requires advance written consent by Solution Provider (which Solution Provider must also obtain from AWS). Customer agrees to cooperate with Solution Provider in transitioning Solution Provider Accounts, and to provide all appropriate information and take all appropriate action necessary to facilitate such transition. In any case, absent prior authorization by AWS, Customer may not transfer Solution Provider Accounts to other providers that are not authorized to resell AWS Services.

5. Proprietary Rights

5.1 Generally. AWS or its licensors own all right, title, and interest in and to the AWS Services, and all related technology and intellectual property rights. Customer (a) has the right to access and use the AWS Services under Solution Provider Accounts solely in accordance with this Access Policy and the Agreement, and (b) may copy and use the AWS Content provided by Solution Provider (or, as applicable, by AWS) solely in connection with Customer's permitted use of the AWS Services. Except as provided in this Section 5, Customer obtains no rights under this Access Policy from AWS, its affiliates, or Solution Provider to the AWS Services, the AWS Content, or Third-Party Content, including any related intellectual property rights. Some AWS Content and Third-Party Content may be provided to Customer under a separate license, such as the Apache License, Version 2.0, or other open source license. By using those materials, Customer is subject to such additional terms. Customer is solely responsible for securing any necessary approvals for the download and use of such materials.

5.2 Restrictions. Neither Customer nor any End User will use the AWS Services or AWS Content in any manner or for any purpose other than as expressly permitted by this Access Policy and the Agreement. Neither Customer nor any End User will, or will attempt to (a) modify, distribute, alter, tamper with, repair, or otherwise create derivative works of any AWS Content or Content included in the AWS Services (except to the extent Content included in the AWS Services is provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the AWS Services or apply any other process or procedure to derive the source code of any software included in the AWS Services (except to the extent applicable

law doesn't allow this restriction), or (c) access or use the AWS Services in a way intended to avoid incurring fees or exceeding usage limits or quotas.

5.3 Suggestions. If Customer provides any Suggestions to AWS or its affiliates, AWS and its affiliates will be entitled to use the Suggestions without restriction. Customer hereby irrevocably assigns to AWS all right, title, and interest in and to the Suggestions and agrees to provide Customer and AWS any assistance required to document, perfect, and maintain AWS's rights in the Suggestions.

5.4 U.S. Government Rights. In accordance with Federal Acquisition Regulation (FAR) Sections 12.211 and 12.212, and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 227.7202-1 and 227.7202-3, the AWS Services are provided (as applicable) as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the AWS Services. If Customer is using the AWS Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Customer will immediately discontinue its use of the AWS Services (including any AWS Content).

6. Representations and Warranties. Customer represents and warrants to Solution Provider that (a) Customer's and its End Users' use of the AWS Services (including any use by its employees, personnel, and (except for Solution Provider) contractors) will not violate this Access Policy, including the AWS Services Policies; (b) Customer or its licensors own all right, title, and interest in and to Account Content; (c) Account Content (including the use, development, design, production, advertising, or marketing of Account Content) or the combination of Account Content with other applications, Content, or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) Customer's use of the AWS Services will not cause harm to any End User.

7. Definitions.

"Account Content" means Content that Customer or any End User (a) runs on the AWS Services, (b) causes to interface with the AWS Services, or (c) uploads to the AWS Services or otherwise transfer, process, use or store in connection with the AWS Services.

"AWS Content" means Content AWS makes available (either directly or indirectly) in connection with the AWS Services or on the AWS Site to allow or facilitate access to and use of the AWS Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Content does not include the AWS Services.

"AWS Services" means, collectively or individually (as applicable), the web services made commercially available by us to Solution Provider for use under this Access Policy, including (as applicable) those web services described in the AWS Service Terms.

"AWS Services Agreement" means the AWS Customer Agreement at <http://aws.amazon.com/agreement>, or other written agreement by and between AWS and Customer (if any) governing Customer's access to and use of the AWS Services.

"AWS Services Policies" means the following provisions (uses of the pronoun "you" shall refer to Customer):

- *AWS Acceptable Use Policy*, located at <http://aws.amazon.com/aup> (as it may be updated by AWS from time to time), which describes prohibited uses of the AWS Services and the AWS Site;
- *AWS Service Terms*, located at <http://aws.amazon.com/serviceterms> (as they may be updated by AWS from time to time), which include the rights and restrictions for particular AWS Services;
- *AWS Site Terms*, located at <http://aws.amazon.com/terms/> (as they may be updated by AWS from time to time), which govern the use of the AWS Site; and
- All restrictions described in the AWS Content and on the AWS Site.

"AWS Site" means <http://aws.amazon.com> and any successor or related site designated by AWS.

"Content" means software (including machine images), data, text, audio, video or images.

“Documentation” means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals, instructions and specifications for the Services currently located at <http://aws.amazon.com/documentation>, as such documentation may be updated by us from time to time.

“End Customer Account” means an AWS account designated as such under the AWS Solution Provider Program, through which AWS Services are provided by Solution Provider to Customer, and in connection with which AWS and Customer have an AWS Services Agreement.

“End User” means any individual or entity that directly or indirectly through another user: (a) accesses or uses Account Content; or (b) otherwise accesses or uses the AWS Services under Solution Provider Accounts. The term “End User” does not include individuals or entities when they are accessing or using the AWS Services or any Content under their own AWS account, rather than Solution Provider Accounts.

“Solution Provider Accounts” means Solution Provider’s AWS accounts through which AWS Services are provided by Solution Provider to Customer.

“Suggestions” means all suggested improvements to the AWS Services or AWS Content that Customer provides to AWS or its affiliates.

“Third-Party Content” means Content made available to Customer by any third party on the AWS Site or in conjunction with the AWS Services.

Exhibit B - Attachment 2

AWS EXCLUSIVE AREA FOR PUBLIC SECTOR SALES IN THE EUROPEAN ECONOMIC AREA

(Last Updated February 24,2023)

Amazon Web Services, Inc. and its affiliates ("**AWS**")* have established an AWS Exclusive Area (as defined below) in the European Economic Area. Active Sales into the AWS Exclusive Area are reserved for AWS itself, as set forth in the agreements between AWS and authorized resellers or providers of AWS-based solutions (collectively, "**Solution Providers**") governing the resale of AWS services (the "**Agreements**"). Unless otherwise defined herein, all capitalized terms used herein will have the meanings set forth in the Agreements.

Solution Providers may not Actively Sell AWS services to Public Sector End Customers** located in the following country (the "**AWS Exclusive Area**")***

Malta

*If a Solution Provider is located in India and the operative Agreement is between a Solution Provider and Amazon Web Services India Private Limited ("**AWS India**"), then all references in this document to "AWS" shall be deemed as referring to AWS India.

** (referred to in some Agreements as "Public Sector Customers")

***The AWS Exclusive Area does not include European Union institutions which may be located in any of the above countries.

EXHIBIT C

SECURITY STANDARDS

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Addendum.

Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

Physical Security

Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the “Facilities”). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo- ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

COUNTY OF SAN MATEO



Jas Sandhar
Procurement Manager

Procurement Division
455 County Center, 4th Floor
Redwood City, CA 94063
650-363-4408 T
jsandhar@smcgov.org
<https://hr.smcgov.org/procurement>

May 4, 2022

Dear Contractor, Vendor, or Supplier:

I am the Procurement Manager for the County of San Mateo, California ("County"), and I write because you have been identified as the contact person for a person or entity that has an agreement with the County of San Mateo (the "County") to provide goods or services.

All County contracts include terms that require contractors to comply with applicable laws while performing under the agreements. As you may know, the United States and State of California have taken action against Russia in response to its aggression in Ukraine, including by imposing economic sanctions. The County is working to ensure compliance with these sanctions and related orders.

Detailed information about the sanctions, including relevant Executive Orders issued by the President of the United States and the Governor of California, may be found at the following websites maintained by the United States and the State of California:

- <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions>
- <https://www.dgs.ca.gov/OLS/Ukraine-Russia>

The County is hereby directing its contractors, vendors, and suppliers, including you, to notify the County if the provision of goods and/or services under any agreement with the County, or payment under any such agreement, is prohibited by these sanctions. If you have reason to believe that the sanctions against Russia prohibit performance or payment under your agreement with the County, please send an email to procurement@smcgov.org with the subject line "Sanctions Against Russia." Please include the relevant contract/agreement number, if you know it, or a copy of the agreement, with your email. Please also include a short explanation of why you have reason to believe that the sanctions against Russia prohibit performance or payment under the agreement.

We greatly appreciate your partnership with the County and your attention to this important matter. Please also keep in mind that failure to comply with applicable law, including the above-referenced sanctions, could result in contract termination.

If you have any questions regarding this correspondence, please do not hesitate to contact the County's Procurement Department at procurement@smcgov.org, or call me at (650) 363-4408.

Sincerely,

A handwritten signature in black ink, appearing to read "Jas Sandhar", is written over a horizontal line.

Jas Sandhar, Procurement Manager